2. SUBJECTNOTESPPTsSELFSTUDYMETIRIALS:

UNIT-1

IntroductiontoCyberLawEvolutionofComputerTechnology:

IntroductiontoCyberSecurityandcyberlaws

Introduction-CyberSecurityBasics:

Cybersecurityisthemostconcernedmatterascyberthreatsandattacksareovergrowing.Attackersarenowusingmoresophisticatedtechniquestotargetthesystems. Individuals,small-scalebusinessesorlargeorganization,areallbeingimpacted.So,allthesefirmswhetherITornon-ITfirmshaveunderstoodtheimportanceofCyberSecurityandfocusingonadoptingallpossiblemeasurestodealwithcyberthreats.

Whatiscybersecurity?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threatreduction,vulnerability reduction, deterrence, internationalengagement, incident response, resiliency, and recovery policies and activities,includingcomputer network operations, information assurance, law enforcement, etc."

OR

Cybersecurityisthebodyoftechnologies,processes,andpracticesdesignedtoprotect networks,computers,programsanddatafromattack,damageorunauthorizedaccess.

- Thetermcybersecurityreferstotechniquesandpracticesdesignedtoprotectdigitaldata.
- Thedatathatisstored,transmittedorusedonaninformationsystem.

OR

CybersecurityistheprotectionofInternet-connectedsystems,includinghardware,software,anddatafromcyberattacks.Itismade up of two words one is cyber and other is security.

- Cyberisrelatedtothetechnologywhichcontainssystems,networkandprogramsordata.
- Whereassecurityrelatedtotheprotectionwhichincludessystemssecurity,networksecurityandapplicationandinformationsecurity.

Whyiscybersecurityimportant?
Listedbelowarethereasonswhycybersecurityissoimportantinwhat'sbecomeapredominantdigitalworld:

- Cyberattackscanbeextremelyexpensiveforbusinessestoendure.
- Inadditiontofinancialdamagesufferedbythebusiness,adatabreachcanalsoinflictuntoldreputationaldamage.

Cyber-attacksthesedaysarebecomingprogressivelydestructive.Cybercriminalsareusingmoresophisticatedwaystoinitiatecyberattacks.

- RegulationssuchasGDPRareforcingorganizationsintotakingbettercareofthepersonaldatatheyhold.

  Becauseoftheabovereasons,cyber securityhasbecomeanimportant part ofthebusinessandthefocusnowisondevelopingappropriate response plans that minimizethe damage in the event ofa cyber attack.

  But,anorganizationoranindividualcandevelopaproperresponseplanonlywhenhehasagoodgriponcybersecurityfundamentals.

CybersecurityFundamentals–Confidentiality:

Confidentialityisaboutpreventingthedisclosureofdatatounauthorizedparties.Italsomeanstryingtokeeptheidentityofauthorizedpartiesinvolvedinsharingandholdingdataprivateandanonymous.

Oftenconfidentialityiscompromisedbycrackingpoorlyencrypteddata, Man-in-the-middle(MITM)attacks,disclosingsensitivedata.Standardmeasures to establish confidentiality include:

- Dataencryption
- Two-factorauthentication
- Biometricverification
- Securitytokens

Integrity

Integrityreferstoprotectinginformation frombeingmodifiedbyunauthorizedparties.Standard measurestoguaranteeintegrityinclude:

- Cryptographicchecksums
- Usingfilepermissions
- Uninterruptedpowersupplies
- Databackups

Availability

Availabilityismakingsurethatauthorizedpartiesareabletoaccesstheinformationwhenneeded.Standardmeasurestog

uarantee availability include:

- Backingupdatatoexternaldrives
- Implementingfirewalls
- Havingbackuppowersupplies
- Dataredundancy

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code toalter computer code, logic or data and leadtocybercrimes, such as information and identity theft.

Cyber-attackscanbeclassifiedintothefollowingcategories:

1) Web-basedattacks
2) System-basedattacks

Thesearetheattackswhichoccuronawebsiteorwebapplications.Someoftheimportantweb-basedattacksareasfollows-

1. Injectionattacks

Itistheattackinwhichsomedatawillbeinjectedintoawebapplicationtomanipulatetheapplicationandfetchtherequiredinformation.

Example-SQLInjection,codeInjection,logInjection,XMLInjectionetc.

2. DNSSpoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced intoaDNSresolver'scachecausingthenameservertoreturnanincorrectIPaddress,divertingtraffictotheattackerscomputeroranyothercomputer.TheDNS spoofingattackscangoonforalongperiod of time without being detected and can cause serious security issues.

3. SessionHijacking

Itisasecurityattackonausersessionoveraprotectednetwork.Webapplicationscreatecookiestostorethestateandusersessions.Bystealingthecookies,an attacker canhaveaccessto all of the user data.

4. Phishing

Phishingis a type of attack which attemptsto steal sensitiveinformation like user logincredentialsandcreditcardnumber.Itoccurswhenanattacker is masqueradingasatrustworthyentity in electronic communication.

5. Bruteforce

It is a type of attack which uses a trial and error method. This attack generates a large numberof guesses and validates them to obtainactualdata like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or bysecurity,analysts to test an organization's network security.

6. DenialofService

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the targetwithtraffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It canbeclassified into the following-

Volume-basedattacks-

Itsgoalistosaturatethebandwidthoftheattackedsite,andismeasuredinbitpersecond.**Protocolattacks-**

Itconsumesactualserverresources,andismeasuredinapacket.

Applicationlayerattacks-Itsgoalistocrashthewebserverandismeasuredinrequestpersecond.

7. Dictionaryattacks

Thistypeofattackstoredthelistofacommonlyusedpasswordandvalidatedthemtogetoriginalpassword.

8. URLInterpretation

ItisatypeofattackwherewecanchangethecertainpartsofaURL,andonecanmakeawebservertodeliver webpagesfor whichheisnotauthorizedtobrowse.

9. FileInclusionattacks

Itisatypeofattackthatallowsanattackertoaccessunauthorizedoressentialfileswhichisavailableonthewebserverortoexecutemaliciousfilesonthe web server by making use of the include functionality.

10. Maninthemiddleattacks

Itisa typeofattackthatallowsanattacker tointerceptsthe connectionbetween clientand serverandactsasa bridge betweenthem.Duetothis,an attacker will be able to read, insert and modify the data in the intercepted connection.

System-basedattacks

These are the attackswhich are intended to compromise a computer or a computer network. Someof theimportant system-based attacksareasfollows-

1. Virus

Itisatypeofmalicioussoftwareprogramthatspreadthroughoutthecomputerfiles without theknowledgeofauser. Itisaself-replicatingmaliciouscomputerprogramthatreplicatesbyinsertingcopiesofitselfintoothercomputerprogramswhenexecuted.Itcanalsoexecuteinstructionsthatcauseharmtothe system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfectedcomputers.Itworkssameasthecomputervirus.Wormsoftenoriginatefromemailattachmentsthat appear to be from trusted senders.

3. Trojanhorse

Itis a malicious program that occurs unexpected changes to computer setting and unusualactivity,evenwhenthecomputershouldbeidle.Itmisleads the user of its true intent. It appearsto be a normal application but whenopened/executed some malicious code will run in thebackground.

4. Backdoors

It isa methodthatbypassesthenormalauthenticationprocess. Adeveloper maycreatea backdoorsothatanapplication oroperatingsystemcan beaccessed for troubleshooting or other purposes.

5. Bots

Abot(shortfor"robot")isanautomatedprocessthatinteractswithothernetworkservices.Somebotsprogramrunautomatically,whileothersonlyexecutecommandswhentheyreceivespecificinput.Commonexamplesofbotsprogramare the crawler, chatroom bots, and maliciousbots.

CyberSecurityandCyberLaws

Astechnologyevolved,theneedtoregulatehumanbehaviorevolvedtoo.Cyberlawscameintoexistenceinordertoensurethatpeopleusetechnologyandavoiditsmisuse.

Ifanindividualcommitsanactwhichviolatestherightsofapersoninthecyberspace,thenitistreatedasacyberspaceviolationandpunishableundertheprovisionsof the cyber laws.

Sincethecyberspaceiscompletelydifferentfromthephysicalworld,traditionallawsarenotapplicablehere.Inordertoprovidecybersecuritytousers,thegovernment introducedseveralcyber laws.

Whentheinternetwasdesignedanddeveloped,thedevelopershadnoideathatitwouldhavethepotentialofgrowingtosuchgreatanextent.

Today,manypeopleareusingtheinternetforillegalandimmoralactivitieswhichneedregulation.Inthecyberspacethingslikemoneylaundering,identitytheft,terrorism,etc.havecreatedaneedfor stringentlawstoenhancecybersecurity.

Additionally,manytechnologicallyqualifiedcriminalslikehackersinterferewithinternetaccountsthroughtheDomainNameServer (DNS),IPaddress,phishing,etc.andgainunauthorizedaccesstoauser'scomputersystemandstealdata.

Whilethereisnocleardefinitionofcyberlaw,itisbroadlythelegalsubjectwhichemanatedfromthedevelopmentoftechnology,innovationofcomputers,useoftheinternet, etc.

CyberLaw:

Cyberlaws, more commonly known as internet laws,are laws thatare relatedto legal informatics,regulating thedigital distribution of information, e-commerce, sofrware, and information security. It usually covers many related areas, such asusage and accessto the internet, freedom of speechandprivacy.

CyberLawencapsulateslegalissueswhicharerelatedtotheuseofcommunicative,transactional,anddistributiveaspectsofnetworkedinformationtechnologiesanddevi es.

Itisnotasdistinct asthePropertyLawor other suchlawssinceit coversmany areasthelawandregulation.It encompassesthelegal, statutory,andconstitutionalprovisionswhichaffectcomputersandnetworks.

Further,itconcernsitselfwithindividuals,andinstitutionswhich:

- Playanimportantpartinprovidingaccesstocyberspace
- Createhardwareorsoftwarewhichallowspeopletoaccesscyberspace
- Usetheirowncomputersandentercyberspace

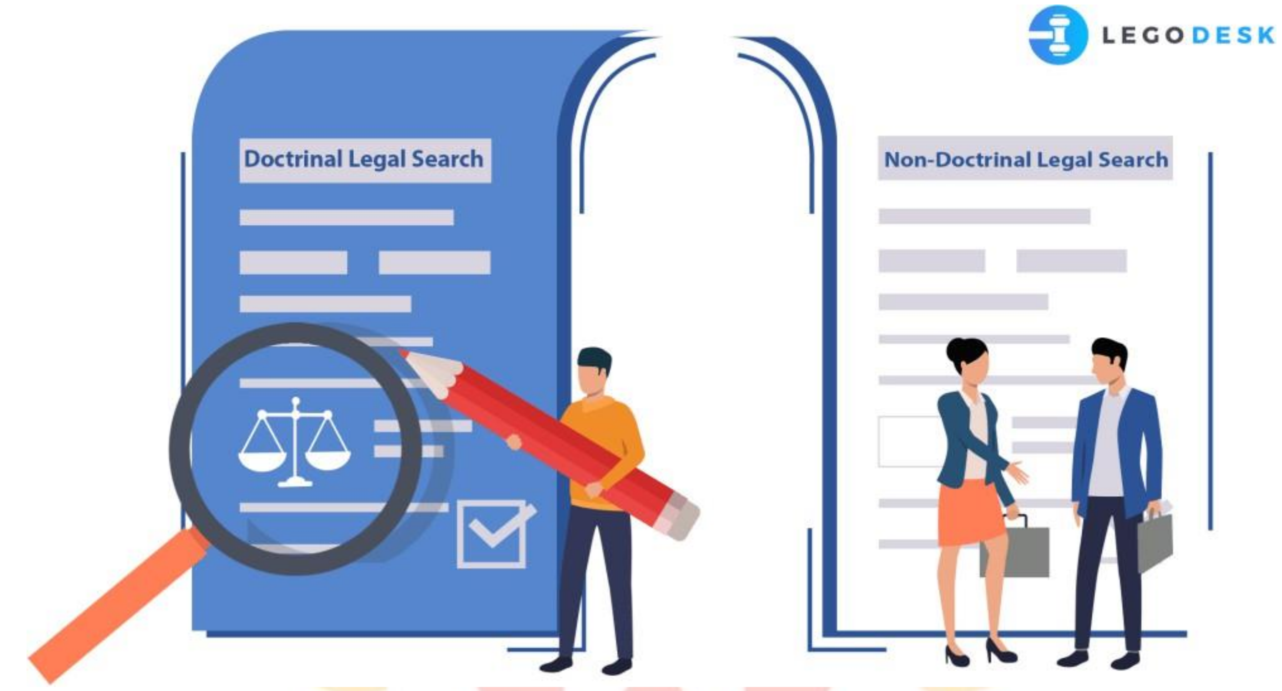
CyberLawisa genericterm referringtoallthelegalandregulatoryaspectsoftheinternet.Everythingconcernedwithorrelatedtooremanatingfromanylegalaspectsorconcerninganyactivitie ofthecitizensin thecyberspacecomes within theambit ofcyber laws.

Whycybercrimelaws:

Many security and privacy issues arise with theuse of theinternet.Ingenious criminal have been known to use advanced strategies to carry outunauthorizedactivities and potential fraud.

What is Doctrinal and Non-DoctrinalWhatdoyoumeanbyLegalResearch?

Legalresearchistheprocessofidentifyingandfindinginformationnecessarytosupportlegaldecision-making.Itisgenerallytheprocess ofcheckingforalegalprecedentthatcanbecitedinabrieforattrial.Virtuallyeverylawsuit,appeal,criminalcase,andthelegalprocess usually requiressomeamountoflegalresearch.Legalresearchskillsareofgreatimportanceforlawyerstosolveanylegalcase, regardlessofareaortypeofpractice.Themostbasicstepinlegalresearchistofindanoteworthycasegoverningtheissuesinquestion.Asmost legal researchers know, this is far more difficult than it sounds.



A researcher’s analysis of acase often begins in theinitialresearch stage when he/sheidentifies therelevant facts and determines the legalissuesthatmustberesearched.Asthisanalysiscontinues,itisfurtherrefinedastheydecidewhere,how,andwhattosearch.When theyfindrelevantlegalmaterials,theymustunderstandthemandhowtheyapplytothefactsoftheircaseinhand.Thisresearchprovidesacrucial analytical foundation that will aid them in their decisions for the remainder of the case.

Whether you are a Lawyer, a paralegal or a lawstudent, it is essential that Legal researchis done in an effectivemanner. Thisis where themethodologycomesintoplay.Differentcasesmustbeapproachedindifferentwaysandthisiswhyitisimportanttoknowwhichtype of legal research methodology is suitablefor your case and helpful for your client.

TherearemanyTypesofLegalResearchlikeDescriptiveLegalResearch,QuantitativeResearch,QualitativeLegalResearch,Analytical Legal Research, Applied Legal Research, Pure Legal Research, Conceptual Legal Research, Empirical Legal Research, Comparative Legal Research, Doctrinal Legal Research, Non-doctrinal Legal Research, etc.

Thisarticletalksin-depthabouttwotypesofLegalResearch:

- **DoctrinalLegalResearch**
- **Non-DoctrinalLegalResearch**

Whatisthemeaningoftheword“Doctrine”underDoctrinalResearch??
DoctrineDefinition: Aruleorprincipleofthelawestablishedthroughtherepeatedapplicationoflegalprecedents.

Commonlaw lawyers usethistermtorefer toan established method ofresolvingsimilar factual or legalissues.For Example**DoctrineofIndoor Management**– (According to this doctrine, persons dealing with the company need not inquire whether internal proceedings relating to the contract are followed correctly, once they are satisfied that the transaction is in accordance with the memorandum and articles of association.)

The word doctrinerefersto aset of beliefs. Theword comes from the Latindoctorfor “teacher,”sothink of a doctrineis theteachings of aschool,religion,orpoliticalgroup.DoctrineanddoctorderivefromthesameLatinword,docere,whichmeans“toteach”:doctormeans “teacher,” and doctrina means “teaching, learning.”

Alegal doctrineis aframework, set of rules, proceduralsteps, or test, often established through precedent in thecommon law, through which judgments can be determined in a given legal case.

Whatisthemeaningoftheword“Non-Doctrine”underNon-DoctrinalResearch?
The word*Non-Doctrine*under Non-Doctrinal Research deals with the Socio-legal aspect of the research. Here, fieldwork is the most important part of the research. Thus scope is wider. It is more concerned with social values. It can be a problem, policy or law reform based. Non Doctrinal research can be qualitative or quantitative or could be part of a large scale project.

WhatisDoctrinalLegalResearch?
Thecentralquestion of inquiryhereis ‘what is thelaw?’ on aparticular issue. It is concerned withfindingthelaw, rigorously analysingit and coming up with logical reasoning behind it. Therefore, it immenselycontributes to the continuity, consistency, and certainty of law.

Thebasicinformationcanbefoundinthestatutorymateriali.e.primarysourcesaswellinthesecondarysources.However, theresearch has its ownlimitations,itissubjective, that islimitedtotheperceptionof theresearcher, awayfromtheactual workingof thelaw, devoid of factorsthat lie outside the boundaries of the law, and fails to focus on the actual practice of the courts.

MethodologyofDoctrinalResearch

Doctrinalorlibrary-basedresearchisthemostcommonmethodologyemployedbythoseundertakingresearchinlaw.Doctrinalresearch asks,whatisthelawinaparticularcase.Itisconcernedwiththeanalysisofthelegaldoctrineandhowitwas developedandapplied.As it is wellknown,thisispurelytheoreticalresearchthatconsistsofeithersimpleresearchaimedat findingaspecificstatementofthelaw,oritislegal analysiswithmorecomplexlogicanddepth.Inshort,itislibrary-basedresearchthatseekstofindthe“onerightanswer”to certainlegalissuesorquestions.Thus,theaimofthistypeofmethodologyistomakespecificinquiriesinordertoidentifyspecificpieces of information.

Forexample,aninvestigationcanbeconductedtofindspecificlegislationthatmonitorsoccurrencesofchildabuseinaparticular jurisdiction.All inquiries will have specific answers tospecific questions that can be easily found and verified, and these arethekeysto is doctrinal or library-basedresearch.Thesesteps includeanalysis of legalissues in order todeterminetheneedfor further research.This stageofteninvolvesagreatdealofbackgroundreadingonasubjectusingsourcessuchasdictionaries,encyclopaedias,major textbooks,treatises,andjournalsthatareaccompaniedbyfootnotes.ThesesourcesprovideDefinitionsofTermsthathelptheresearcherunderstand and summarize the legal principles involved in the field of law understudy.

NormativeCharacterofDoctrinalResearch

The normativecharacter of doctrinal research inparticular contexts, is concerned with the discovery and development of legal doctrines and research, for publication in textbooks and journals that take theform of asking the question, “What is thelaw?”

Legalrulesarenormativeincharacterbecausetheydictatehowweshouldbehaveasindividuals.Theymakenoattempttoeitherexplain, predict,orevenunderstandhumanbehaviour,justtodescribeit.Inshort,doctrinalresearchisnottherefore researchaboutlawatall.In asking “What is thelaw?”it takes theinternal cognitive approach orientedto the aim of thestudy. For this reason, it is sometimes described as research in the field of law.

WhatisNon-DoctrinalLegalResearch?

Non-doctrinalresearch, alsoknown as social-legal research,is researchthat employsmethods takenfrom other disciplines togenerate empirical datathat answers research questions. It can bea problem, policy, or areform of theexisting law. A legal non-doctrinalfinding can be qualitative or quantitative, and a dogmatic non-doctrinal finding can be part of alarge-scale project. Thenon-doctrinal approach allows the researcher toconduct research that analyses the lawfrom the perspective of other scientific disciplines, and to employ those disciplines indraftingthelaw. Forexample, inthebehavioural sciences,thereis astandardform ofaconsumercontractthatcontributes to the study of psychological phenomena:

1. Thetendencyofconsumersnottoreadthestandardformcontract,
2. Theinabilityofconsumerstoevaluatethetermsofthecontractcorrectlyoncetheydoread.And
3. The ability of sellers to deal with consumers. Because it uses non-sectarian legal experimental data, it provides vital insights about thelawin context, i.e. howthe lawworksout inthe real world. Legal research isexperimental and valuable in detecting andexplainingpracticesandproceduresinlegalandregulatorysystems.Itisalsovaluableinsettlingdisputesandimpacts the legal phenomenaofsocialinstitutionsandbusinesses.Similarly,experimentallegalresearchineconomicsapplieslegal analysis,statisticalinference,andeconomicmodelling,tothecoreareasofnationalandinternationallaw,suchastort,property,contracts,criminallaw,lawenforcement,andlitigation.Earlierresearchcanbeusedtoanalyzetheeconomicsoflegal negligencetheory.

Consequentialapproch:Definition&Examples

Summary

- A consensus theory is one which believes that the institutions of society are working together to maintainsocial cohesionandstability.

- Value consensus assumes that the norms and values of society are generally agreed upon and that social life is basedoncooperation rather than conflict.

- Consensus theories have a philosophical tradition datingback to Plato andRousseau, who arguedforstructures thatmaintainthe consensus of society.

- The first formal sociological consensus theory, however, is EmileDurkheim's Functionalism, which argues thatallinstitutionswithin a society serve an essential purpose.

- Others, such as Merton, elaborated on Durkheim"s functionalist theory, adding that institutions can also bedysfunctional.Nonetheless, these theories are still consensus theories.

- More recently, consensus theories have been extended into pluralism and the "new right." Pluralism argues thatdifferentgroups,orsubcultures, withinsociety, canhave differingnormsand values, buttherearealeastsome overriding,sharedsocietalnorms.

- Meanwhile, the new right emphasizes how the breakdown of social institutions can harm society through the dismantlingofvalueconsensus.Criminologistsalsocommonlyuseconsensustheories.Onenotableexampleofacriminologicalconsensustheory is strain theory.

Definition

Thetermconsensusmeansagreement.Itisusedinsociologytodescribetheoriesthatstresstheessentialcohesionandsolidarityofsociety,wherethe core principle of social life is an agreement or the mutual cooperation of the members of a society.

These theories see common experiences, interests, and values as the defining characteristic of a population or a society. For example,aconsensus theorist may study sports as a source of binding people together in a shared experience or the role that education playsininstilling shared norms and values.

Thereisusuallyalegitimateauthorityinvolvesinpolicingtheconsensus,whichalsoguaranteesthatsocietiestendtopersist.

Consensustheoryisoftencontrastedwithconflicttheory.ThisperspectivewasfirstdevelopedandpopularizedbytheHarvardUniversitysociologistTalcottParsons(1939,1951),whobelievedthattheequilibriumofsocialsystemsandtheintegrationofvariouselementswithinthem were thefoundations of social systems.

Consensustheoriesoftenserveasasociologicalargumentforthefurtheranceandpreservationofthestatusquo.Intheviewofconsensustheories,rules are set and inherently functional; whoever does not respect them is, by default deviant.

ExamplesOfConsensusTheories

A consensusapproach refers to sociological theories that argue thatsome overriding consensus as to the norms andvalues of asocietyisessential for its function.

According to consensus theories, these agreed-upon norms and values are inherently functional and beneficial This means thatwhensomeone in society counters these norms and values, they are behaving delinquently.

Consensus-like theories have a philosophical tradition dating back to Plato and Rousseau, who argued for structures that maintaintheconsensus of society. The firstformal sociological consensus theory, however, is Emile Durkheim's Functionalism, which argues thatallinstitutions within a society serve an essential purpose.

Others, such as Merton (1957), elaborated on Durkheim"s functionalist theory, adding that institutions can also bedysfunctional.Nonetheless, these theories are still consensus theories.

More recently, consensus theories have been extended into pluralism and the "new right." Pluralism argues that different groups,orsubcultures, within society can have different norms and values, but there are at least some overriding, shared societal norms.

Meanwhile,thenewrightemphasizeshowthebreakdownofsocialinstitutionscanharmsocietythroughthedismantlingofvalueconsensus

Criminologistsalsocommonlyuseconsensustheories.Onenotableexampleofacriminologicalconsensustheoryisstraintheory.

5DifferentApproachestoMaintainingCyberSecurity

Cybersecurityin2021isveryimportant.Itisbecominganecessityforbusinessestohavestrongsecuritysolutions.Today,itisnotagood securityapproachtousejustonesecuritytool.Enterprisespayhugefinesorgooutofbusinessbecauseofsimplesystemhacks.AccordingtoForbes, cybersecurity is crucial to both small startups and large corporations.

Cybersecurityisnotplug-and-play.Itdemandsinvestmentinvarioustoolsalongsideakeenfocusontrainingandcustomizationoftools and integration to realize the return on investment.

Since every company is a technology company, the stakes are very high. Technology is no longer a supplement to business operations since, in most cases, digital assets are at the core of business operations.

Tohelpcurbsecuritythreats,thisarticlehighlightsfivedifferentwaysofpreventingcyberattacks.

WhatisCyberSecurity?

It is the protection of networked systems such as data, software, and hardware from cyber threats. Both enterprises and individuals rely on this practice to protect computer systems and data centers from unauthorized access.

Arobustcybersecurityapproachcanwithstandmaliciousattacksaimedataccessing,altering,deleting,destroying,orextortingauser'sor organization'ssystemsandvaluabledata.Also,cybersecurityisimportantinthwartingattacksdesignedtodisruptordisabletheoperationsofa system.

ImportanceofCyberSecurity

The increasing number of programs,devices, and users inmodern enterprises, coupled with increased confidential and sensitive data,increases the importance of cyber security.

Also,thegrowingnumberandcomplexityofcyberattacktechniquesincreasetheneedforrobustcybersecurity.

ApproachestoMaintainingCyberSecurity

Across all enterprises, maintaining cyber security within a constantly changing threat landscape is a big challenge. Traditional reactive approaches are no longer sufficient. To acclimatize to the evolving security threats, businesses need more proactive and adaptive approaches.

Automatingroutinesecuritytasks

Today,security automationrelies on software-based processes to investigate, detect, and fix threats to systems and applications. It can take place with or without manual input. When used in conjunction with existing security measures, automation assists in establishing incoming cyber threats, prioritizing remediation, and offering actionable information to security teams for faster response.

Security automation is a process that connects tools and solutions for finding and fixing vulnerabilities in software. When development andsecurityteamsautomatetheidentification, prioritization, andremediation, theycanpayattentiontochallengingaspectsof ensuring the deployed application remains secure.

Since hackers target applications more often, a manual response is usually labor-intensive and slow. However, automating application security provides an easy and repeatable process that ensures the technology environment of a business remains secure. In realizing automated security, the best application security practices recommend relying on various automated tools in each development phase.

SecurityProcessesThatcanbeAutomatedAutomationcanmanagethetediousandcrucialaspectsofacybersecurityframework.Belowarethefiveprocessesthatcanbenefitfrom securityautomation.

- **Monitoring and detecting threats:**Businesses should be able to see all the areas of the IT environment all the time. Security monitoring tools offer such visibility at scale and can monitor any detected threats. Some automation tools are capable of monitoring open-source code in applications during production and notifying security teams when they detect vulnerabilities.
- **Investigating threats:**After establishing a vulnerability, security automation can discover affected nodes or machines, the level of damage, and the vulnerability exploited. Compared to security teams, security automation accomplishes this forensic task much faster thanengineersordevelopers.Forinstance,incaseofadenialofservice(DoS)attack,securityautomationcanestablishifitwascausedbymisuseoran abrupt HTTP flood. The details help establish the necessary remediation or protection.
- **Respondingtoincidents:**Securityautomationprovidesaquickwayofrespondingtoincidents.Ithelpsremovemalware,deactivatea service or install upgrades or patches as safeguards against new attacks.
- **Permissionmanagement:**Oneofthekeycybersecuritytasksinvolvesmanagingusersandpermissions.Ifasystemhasthousandsofusers,it isachallengeto doit manually. However,automatingthe process of provisioninganddeprovisioning ausersaves alot of resourcesand time.
- **Applicationandbusinesscontinuity:**CybersecurityautomationcanrelyonIPblockingincaseofabruteforceattacktoavoiddamage whileallowingotherIPaddresses.Inaddition,automationcanreplicateessentialserverinstances,whichhelpsensurecriticaldataisalways available.

Educatingandtrainingusers

Foranyorganization seriousabout maintainingcybersecurity, employee trainingwill be part of itsDNA. Often, data breachesarise from human psychological weaknesses. So, having a good security training curriculum for employees goes a long way in maintaining cyber security and protecting assets and data.

Thecurriculumshouldincludeawarenesstrainingtargetingemployeesanddeveloperstocarryoutcoding.Organizationsshoulddosuch trainingregularlyinsteadofdoingitonceperyear.Also,conductsimulationssuchasphishingteststoassistemployeesinidentifyingand stopping socialengineeringattacks.Suchtraininghelpsemployeesestablishwarningsignsofasecuritybreach,safepractices,andwaysof responding to a suspected attack.

DocumentsecuritypoliciesHaveaknowledgerepositorythatcontainscomprehensivesoftwaresecuritypolicies.Thesecuritypoliciesletemployeessuch asnetwork administratorsandsecuritystaffunderstandtheactivitiestakingplaceandwhy.However,itisnotenoughtohavepolicies.Organizationsshould ensureeverybodyreadsthem.Also,itshouldbepartofonboardingnewemployees.

Networksegmentation

Segmentinga companynetwork entailsapplyingthe principle of least privilege. With appropriate network segmentation, businesses can limit the movement of attackers. It starts by establishing where critical data is stored and using appropriate security controls that limit traffic in and out of such sensitive network segments.

Monitoringuseractivities

Althoughorganizationstrusttheiremployees,theyhavetoverifyemployeesare adheringtothebestsecuritypractices.Thus,monitoring helps detect suspicious operations like privilege abuse or user impersonation.

Maintainingcybersecurityaimstoensureanorganization'sdataremainssafefrombothexternalandinternalbadactors.Itcombinesthe use of technologies, practices, processes, and structures to safeguard data, computers, and software from unauthorized access.

3ProactiveApproachestoCyberSecurity

Cybersecurityiscriticallyimportanttoeveryorganizationand,asasecurityprofessional,itisyourdifficultjobtoensurethatcompanydataissafe.Butwhat are bestand most current waystokeep information secure? Here we look at three of the best proactiveapproaches to cybersecurity.

1. **ThreatDetection**

Threat detection is one of the most innovative and effective ways to stay on top of cyber criminals. This collaborative approach isan innovativewayforthecommunityofcybersecurityprofessionalstopoolresourcesandinformation, stayingonestepaheadofhackers. Threatintelligenceisyourbestadvantage over loss of data, finances, and public trust. Threat intelligence provides real-world, real-time information onadversaries, threats, andmaliciousattacks.

More and more businesses across all industries are implementing threat intelligence programs in their organizations. The development processiscritically important to ensure that you are receiving relevant and prioritized threat data that is valuable for your organization. Working with the**rightpartner**when embarking on this process will help save you time, money, and stress.

2. **DPM5GLReal-TimeCompliance**

The need for real-time info is critical. According to cybersecurity expert Larry Karisny, author of**Will DPM 5GL Save Cybersecurity?**, "Wemustmove forward from historical analysis to real-time 5GL event patterns if we are to successfully monitor data-in-motion activities. This is whereandhow we must deploy new cybersecurity technologies to truly defend ourselves against cyberattacks."

DPM 5GLstandsforDigitalProcessManagement5thGenerationProgrammingLanguageanditisdesignedtodetectanomaliesfromregularpatterns.By relyingon patternanalysisrather thanalgorithms, DPM 5GL allows for real-timeauditandanalysis. Ifit always seemslikehackersare one stepaheadof you,it is becausetheyusually are. This protocol attemptsto level the playing field by mitigatingthetypical advantages that hackers have.

3. **Encryption**

Encryption is like your oldest cybersecurity friend. It may not be the newest approach, but it certainly has its advantages.Cryptographicalgorithmshave long been usedin security protocols, and many current products still support older encryption measures.

Thepreviousgo-to56-bitDES hasbeenreplacedwith128-bit AdvancedEncryptionStandard(AES)that provides stronger security.Now, thereisnextgeneration encryption, which willenableeven betterscalabilityand easiergrowth forthefuture. Thenext gen ofcryptographyhasemerged fromthesestandards through 30 years of global development and study. Thereare four categories of AES crypticalgorithms: symmetric key, publickey,ellipticcurve, and hash.

Used bytheU.S.governmentand endorsed bytheNationalInstituteofStandardsandTechnology, AESprotectsclassifiedinformation.Thisstandardisalsoimplemented in software and hardware throughout the world to encrypt sensitive data.

Regardless of which method, or methods, of cybersecurity you chose, it isimperative that you are proactive in your approach. Cyber criminals liketostay on the cutting edge and securityanalysts must stayright onthat edge with them in order to truly protect sensitive data.

CybersecurityEthics:
Cybersecurityethicsgrowsinurgencyasthedigitallandscapecontinuestotransformsociety.Whatshouldcybersecurityprofessionals —thefront-linedefenseagainstthreats—knowaboutcybersecurityethics?

Cybersecurity capabilities have improved thanks to advancements in security technology and heightened awareness of threats. At the same time, however, cybercriminals have become more sophisticated in identifying and attacking weak points. For example, phishing, oneoftheoldestcybercrimes,datingbacktothe1990s,continuestoexpandasathreat.SecurityfirmLookoutreportsthattherate ofmobilephishingwashighestin2022.Also,phishingwasoneofthe most commonattacksusedininternetcrimes,causingmore than $4 billionin losses, in 2020, according to the FBI.

Cybersecurityethicstakescenterstageascybersecurityprofessionalsvieforanedgeovercriminals.Understandingtheethical implications oftheirworkand choicesiscrucialto helping cybersecurity professionalsbalance securitywith other societalvalues.

What'sCybersecurityEthics?

Ethics defines right and wrong actions in specific situations and is fundamental to society. In the cyberrealm, ethics serves as a guidepost for cybersecurity professionals. It helps identify the type of online behavior and conduct that harms individualsand businesses.

Ethical principles are what separate cybersecurity professionals fromhackers. For example, while the latter tries to steal data, the formertries to protect it.When hackers access data, they use it fornefarious purposes. On the otherhand, cybersecurity professionals, who have access to the same data,use their skills to ensure that the data's safe and secure.

ImportanceofCybersecurity

Fromdatabreachesto deepfakes,cybersecurity professionals dealwith many threats.These unethicalonline activitieshave a profound impact on people and business. For example, a hacker may steal a company's data, an act that can compromise customer data.A cybercriminal can then take that data and sell it on the darkweb. Cybersecurity is vital to preserve privacy and guard against identity theft.

Cybersecurity also protects people from cybercrimes such as financial fraud. For example, consumers exchange their data withbanks and financial institutions when conducting online banking. Cybersecurity helps secure financial transactions, safeguarding bankaccounts and credit card information.

A breach can also disrupt regularbusiness operations andinconveniencecustomers and employees — or even put regional or national infrastructure atrisk.In urgentsettings, suchashospitals,attackson computer networks can harmpeople and impacttheirhealth.

EthicalResponsibilitiesofCybersecurityProfessionals

Organizations hire cybersecurity professionals to protect their sensitive information from cyber threats, and hiring decisions for cybersecurityrolesdon'tcomelightly.Frameworksforcyberethicsandcodesofconductmayvarybyorganization. What'sthesame is that employers look tohiretrustworthyprofessionals with astrong ethical compass because cybersecurity professionals have access to the same data that cybercriminals wish to steal. The difference is that cybersecurity professionals adhere to cybersecurity ethics, meaning that organizations can trust them to oversee valuable information.

TypesofCybersecurityEthicalIssues

For cybersecurityprofessionals,keepingsystems secureoftenmeansusingprivileged accesstodatatoperformactivitiessuch as whitehat hacking, alsoknown as ethical hacking.Whitehat hacking describes penetrating protected systems using hackingtools andtechniques totest thesecurity of systems, networks andsoftware. Theaim is toidentifysecurity vulnerabilities. **Cybersecurityresearch**tolearn how tobreakthroughthe safeguardsofa systemenablescybersecurityprofessionalstobuilddefensesagainst them.
White hathacking offersan exampleofcybersecurityethicalissuesin theprofession.Awhitehathacker mustbe trustworthyenough to safeguard the confidentiality of the information they encounter, but there have also been notable incidents in which security professionalsdiscoveredcrimesorpublicthreatsthattheydecidedtosharewithauthorities.Asolidethicalfoundationcanserveas the bedrock to help employeesmake the rightdecisionsasthey face some key cybersecurityethicalissues,aslisted below.

HarmtoPrivacy

Harmtoprivacyreferstoanindividual'sprivacybecomingcompromised.Negativeconsequencesincludeunauthorizedaccess, identitytheft,reputationaldamageanddistress.Acybersecurityprofessional'sdecisionsultimatelyimpactprivacyprotection.They can safeguardprivacyinseveralways,includingimplementingsecuritymeasures,toolsandpractices;callingoutdesignsandappsthat misleadusersinto sharing excessive information;ensuring compliancewith security frameworks;and mitigating risks.

HarmtoProperty

Harmtopropertyreferstodamagetobothphysicalanddigitalassets.Itcanleadtounauthorizedaccessandthedisruptionofservices. Foracybersecurityprofessional,prioritizingnetworksecurity

becomes an ethicalmatter.Theyhavearesponsibilitytoimplement countermeasures,whichcaninclude riskassessments,firewallsand continuous monitoring. Failure to do so can lead to property harmcaused by a cyber attack.

CybersecurityResourceAllocation

Determiningwhattoinvestincybersecurityactivitiescanbeachallenge.Largecompaniescaninvestmoreresourcestoenhancetheircyber defenses,improving their chances of detecting anomalies or intrusions. More important, knowinghow to allocate resourcesis essential. Cybersecurity professionals must properly use resources for the greater goodof the organization and its stakeholders. Deploying a patch for a critical software vulnerability may be costly and time consuming, but notdoing so may riska data breach that impacts millions of customers.

TransparencyandDisclosure

Companiesshouldpromptlyrevealcriticalvulnerabilitiesintheirsoftwareuponlearningaboutthem.Thislevekoftransparencycan not only help cybersecurity professionals collaborate and share information to respond quickly to attacks but also allow customerswhosedataisthreatenedtotakeappropriateactiontodiminishtheirownrisks. Approaches to transparency and disclosure depend ontheorganization.However,therecentConsolidatedAppropriationsActof2022 offersguidance:Section2242notesthatcompaniesshouldvoluntarilydiscloseaknowncyberattackwithin72hoursafteritsdiscovery.

EthicalChallengesFacedbyCybersecurityProfessionals

Fromkeepingsensitivedataconfidentialtoconfrontinguserprivacyissues intheworkplace,cybersecurityprofessionalsmust find ahealthy balance between safeguarding information and upholding cybersecurity ethics standards.

Confidentiality

Cybersecurity professionals handle sensitive information, from personal customer data to a business's proprietary information. Disclosing thisdata canhave severeconsequences,so cybersecurityprofessionals mustneverreveal confidential information,unless a significant public benefit exists for doing so.

ThreatsandRisks

Cybersecurity professionals are duty-bound to respond to cyber threats. Remaining vigilant is always a priority, and their response is crucial. Whileindividualsmayoverlooknotificationsorleavetheircomputersunattended, cybersecurityexpertsshouldneverdoso.

BalancingSecurityWithBusinessInterests

Cybersecurity professionals may encounter unethical practices within a business unit. Reporting the issue to supervisors maybe the bestfirststep.Inthe caseofillegalactivity,acybersecurityprofessionalmayconsiderreportingittoauthoritiesorthe media.

UserPrivacy

Cybersecurity professionals have to balance security and user privacy. In protecting their organizations from cyber attacks,cybersecurityprofessionalssometimeshavetoaccessemployees'onlineactivities.Withoutcarefullyconsideringuserprivacy,this can come close to violating a person's rights.

PromotingEthicalPracticesinCybersecurity

Cybersecurity professionals often have unique access to sensitive data. They're responsible for defending this data against malicious actors. This requires an understanding of ethical practices. However, thecyber realm often blurs the linebetween security and privacy, making it imperative for professionals to have clear codes of conduct and demonstrate trustworthiness.

By staying updated on evolving cybercrimes, enhancing competencies and pursuing advanced education, individuals can develop cybersecurity strategies and strengthen their knowledge of ethical principles.

With a curriculum that includes courses in human factors in information security and risk management,**Augusta UniversityOnline'sMasterof Science(MS)inInformationSecurity Management**preparesgraduatestoaccelerate their**cybersecurity careerpaths**. Asolidfoundationofcybersecurityethicsknowledgecanequipcybersecurityprofessionalstoadvancetheircareersinthiscritical field.

CyberJurisdiction:

Afast-pacedworld,andsurprisinglyfittinginone'shand.Theworldisintheeraof"internetandcyberspace",anditseemsfasterandbetterthanever.Butitallcomeswithaprice,thatmankindisstillintheexplorationof.Justasintherealandphysicalworld,thevirtualspacecreatedbyhumansalsoseesaplethoraofcriminalactivitiesonadaytodaybasiswherethedataofmillionsofpeopleactsasvaluableassets.Ithasthepowertoinstigateacivilwarortodestroynationsaltogether,stealdataforransom,orevenrobmillionsfromabankinseconds.Itbecomesquiteachallenge to mapout a conclusive set of applicable laws to containthis mass virtual force. The major obstacle beinghow, whentheseoffencesare prosecuted, the personal jurisdiction is to be applied.

Thisarticlebreaksdownhowthelegalprincipleshaveevolvedwhiledeterminingpersonaljurisdictionincyberspace.

Cyberspace-TheVirtualUniverse

Cyberspaceisanimaginaryareaoravirtualspacewhereaconnectioncanbeestablishedbetweentwocomputersatanytwopointsintheworld, with absolutely no limits.

Theword'cyberspace'wasusedintheNovel**'Neuromancer'byWilliamGibson**,forthefirsttimein1984,whichisasciencefictionanddefined as an interaction between the human mind and computers. 1

Whilecyberspaceandtheinternetshareverysimilarconnotations,cyberspacecanbedefinedasanythingthatisdoneusingtheinternet,whiletheinternet is a network or networks.

Inlayman terms "cyberspace"is a virtualuniverse madeupofthe widely spreadand interconnecteddigital gadgets andtechnology, enablingoneto create, modify, share, exchange, extract and destroy the physical resources floating all over the internet.

Theworldweliveinispossiblyatitssimplest,mostsophisticatedversion,asatthispointintime,andwecouldonlyhopeforittomakemanyinnovativenewchanges.Theworldseemssomuchsmalleratourfingertips,liveshavecollectivelybecomeeasier.Education,E-commerce,shopping,banking,andalmosteveryotheressentialhastakenitsspotontheinternet.Infact,someoftherichestmultinationalcompaniesare thatofGoogleandFacebookthatareempiresbuiltvirtuallyonnothingbutdata.Thehugenumberofusersarethecustomersandtheirpersonalinformation, theasset.Eachofthesebusinessesrunonnothingbutloadsofinformation,someprivate, somenot, anditbecomes necessary tobuildahyper-vigilantscreeningprocessinprovidingourpersonalinformation,becauseoftheimmensethreatsthattag-alongwiththismightytool.

With business transactions moving online, the conventional methods of dealing with legal complications are also in need of remoulding tofitinto the present, needful circumstances.

Itisoftenveryambiguoustodecipherwhatplaceholdsjurisdictionoverdisputesthatariseinthevast

cyberspace.Inherpaper“PrinciplesofJurisdiction”,BetsyRosenblattstatesthat“acourtmust firstdecide“where”theinternetconducttakesplace,and what it means for internet activity to have an “effect” withina state or a nation”. [1]

The concept of national borders and distance stands irrelevant in cyberspace. By setting up a website from a home computer, here inIndia,one can grant access to anybody around the world, making communication a piece of cake. While communication is easier, the legalthreatsposed are quite drastic.

ThreatsToCyberspace

Withtheamountofinformationbeingconstantlyexchanged,thethreatsincyberspaceareequallylarge.Itisalsoimportanttoregistertheintensity of changes the cyberspace is constantly subjected to, which concurrently aids in the advancement of the cyberattacks.

Cyberattackscanrangefrompersonaldatabreachestomassfrauds,eachofwhichisequallydangerousandharmful,puttingone’susageofcyberspac eatrisk.

Cyberattacksarewhereinternetusersusemaliciousmaneuvrestosteal,destroy,expose,orgainunauthorizedaccessintothepersonalinformation of a person, company, military databases, etc.,

Cyberattacksareapartofcyberwarfare-wherecyberspacescontainingclassifiesmilitaryinformation,areattackedtowagewarandothermilitary purposes, and cyber terrorism- where cyberspaces are used to conduct violent criminal activities.

Someofthesecommoncyberattacksincludephishing,identitytheft,ransomware,hacking,childpornography,malware,creditordebitcardfrauds, disinformation- harming an individual, property or a nation.

WhatIsPersonalJurisdiction?

Personaljurisdictionreferstothejurisdictionexertedbylaw,overapersonindecidingaparticularlawsuit.Italsooperatesalongwiththedueprocedureof law establishedby the constitution of that country. Personal jurisdictionincyberspace has evolved, one case law ata time, likecyberspaceitself. The advancements are constant; hence it proposes a challenge for the laws to keep up with it.

Duetoitsversatileandinconsistentnature,absenceofphysicalboundariesanddynamicspacestructures,containingcyberspaceintheboundsofafewspecific laws and assigning jurisdiction becomes quite a task.

Tobreakit down,a“cyberspace”iscreatedbyacomputer,andthisvirtual space “holds”allinformation.Allphysicaltransactionsandalllegalconnotations attached to it goes into overdrive in cyberspace.

“Atransactionincyberspacefundamentallyinvolvesthreeparties.Theuser,theserverhostandthepersonwithwhomthetransactionistakingplacewiththeneedtobeputwithinonejurisdiction.”[2]

In terms of personal jurisdiction, to separate disputes into domestic or international, in cyberspace, it is important to distinguishdisputesbased on (i) what has happened? (ii) where has it happened? (iii) why did it happen?

Hence,aresidentshallinevitablybetriedundermunicipallaws,buttherepersistsambiguitywhiledealingwithnon-

residents.Traditionally,jurisdiction is exerted by a court in specific matters by terms of territory, subject matter, or the applicable law.

Ofteninvolvingmultiplecountriesinone single transactiononcyberspace, it is challengingto dissectthe disputesarising into thelawsofoneparticular country. One ofthe ultimate recourses couldbe sought under Public InternationalLaw, to eliminate jurisdictionalclashesbetweencountries andconflicts of law arisingout of it, usingthe principlesof “personal jurisdiction”. Jurisdiction, under International Law isofthreetypes:(1)

jurisdictiontoprescribe;(2)jurisdictiontoenforce;and(3)jurisdictiontoadjudicate.Toreplicatetheseintocyberspace,onecanconsiderthe‘law ofthe server’, that is, the physical position of the server or where the webpage is located and claim the jurisdiction of thatcountry.However,these principles are of no use when the cyberspaces are used to commit terrorist activities hence maintaining anonymity of itsservers.

PersonalJurisdictioninCyberspaceAroundtheWorld

The UnitedStates, havingoneof the strongestcyberspace laws inforce, whileformulatingprinciples todealwithcases ofcyberspaces, stoodbytheconceptof'minimumcontacts',astandardthatwasoutlinedbytheCourtinInternationalShoevWashington,1945.TheCourtruledthatanon -residentofastatemaybesuedinthatstateifthepartyhas'certainminimumcontactswith[thestate]suchthatmaintenanceofthesuitdoes not offend traditional notions of fair play and substantial justice.'[3]

TheUSSupremeCourtlaterlaiddownthe"Zippertest"orthe"SlidingScaletest"that- "Intheabsenceofgeneraljurisdiction,specificjurisdictionpermitsacourttoexercisepersonaljurisdictionoveranon-residentdefendantforforum-relatedactivitieswheretherelationshipbetweenthedefendantandtheforumfallswithinthe'minimumcontacts'framework"andclassifiedwebsites as (i) passive, (ii) interactiveand (iii) integral to the defendant's business.

The difficultyexperiencedwiththeapplicationofthe Zipposlidingscale testpavedthewayfor theapplicationof"theeffectstest". Thecourtshavethus moved from a 'subjective territoriality' test to an 'objective territoriality' or 'the effects test' inwhich the forum court willexercisejurisdictionifitisshownthateffects ofthe defendant'swebsiteare feltinthe forum state. Inother words,it musthave resultedinsomeharmor injury to the plaintiff within the territory of the forum state- as pronounced primarily in Calder v. Jones.

The recent lawsuit by the International League Against Racism and Anti-Semitism and the Union of French Law Students againstYahoo!,(Yahoo!Inc., v La Ligue Contre Le Racisme Et L'Antisémitisme), whichhas receiveda lot of attention in the popular press summarizesthedifficulties that remain in resolving both the prescriptive and enforcement jurisdictional issues in cyberspace.

Itappearsthatcourtsandlegislatureshavefoundlegitimategroundsforassertingprescriptivejurisdictionoverdefendantsbaseduponactionstakenincyberspace,butthatmayhavelittleimportancewhentheplaintiffseeksarestorativeremedy.Enforcementjurisdiction,whichrequirestheinjuredpartyto attacheitherthedefendantorhistangibleassets,becomesanissueofcomityorstate'srecognitionofitsobligationtoenforce a law. [4]

"In sum,underU.S.law.ifitisreasonabletodoso,acourtinone statewillexercisejurisdictionoverapartyinanotherstateorcountrywhoseconducthassubstantialeffectsinthestateandwhoseconductconstitutessufficientcontactswiththestatetosatisfydueprocess.Becausethisjurisdictionaltestisambiguous,courtsineverystateoftheU.S.maybeabletoexercisejurisdictionoverpartiesanywhereintheworld,basedsolely on Internet contacts with the state."[5]

InEuropeancountries,thejurisdictionofcyberspaceisdeterminedbytheBrusselsRegulationsbyextendingitsoperationstoonlinedisputesandstatesthat"subjectto theprovisionsofthisRegulation, persons domiciledinacontractingstateshall,whatevertheir nationality,besuedinthecourtsofthat state"- thus eliminating the ambiguity of jurisdiction.

GermanyhaspassedalawthatsubjectsanyWebsiteaccessibleinGermanytoGermanlaw,holdingInternetserviceproviders(ISPs)liableforviolations of German content laws if the providers were aware of the content and were reasonably able to remove the content.[6]

Malaysia's new cyberspace law also extends well beyond the borders of Malaysia. The bill applies to offenses committed by a person inanyplace, inside or outside of Malaysia, if at the relevant time the computer, program, or data was either (i) in Malaysia or (ii) capable ofbeingconnected to or sent to or used by or with acomputer in Malaysia. Theoffender isliable regardlessof his nationality or citizenship. [7]

PersonalJurisdictioninCyberspace-TheIndianMechanism

CasioIndiaCo.Limitedv.AshitaTeleSystemsPvt.LimitedtheSupremeCourtheldthat"thewebsiteofDefendantcanbeaccessedfrom DelhiissufficienttoinvoketheterritorialjurisdictionofthisCourt".[8]

In India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors., it was held that "the Defendant is carrying onactivitieswithin the jurisdiction of this court; has sufficient contacts with the jurisdiction of the court and the claim of the Plaintiff has arisenas aconsequence of the activities of Defendant, within the jurisdiction of this court".

InBanyanTreeHolding(P)Limitedv.A.Murali KrishnaReddy,TheDivisionBenchoftheDelhiHighCourt,whileansweringthereferralorderof thelearned Single Judge, affirmed the ruling in India TV, and overruled the Casio Judgement.[9]

VariouslawsinIndiacanbedeemedapplicabletotoday'sscenarioofcyberspaceandeverythingthatisinvolvedwithit.Itisfascinatingtonoticehowsomeoftheselaws,thoughdecadesold,standaccuratetotoday'scircumstances.

BasedontheSections15to20oftheCodeofCivilProcedure,1908,stipulatingtheIndianapproachtodeterminingjurisdiction,thejurisdictionshall bedetrimental to the location of the immovable property, or the place of residence or place of the workof the defendant or theplacewhere thecause of action has arisen. These provisions stand inapplicable for cyberspace disputes.

TheprovisionsoftheCodeofCriminalProcedure,1973prescribesformultipleplacesofjurisdictionbasedontheplaceofcommissionofcrimeoroccurrence of the consequence of a crime in cases of a continuing crime,which, in the case of cyberspace, stands accurate.

ThepersistinglawsrelatingtocyberspacearedealtundertheInformationTechnologyAct,2000,inIndia.TheobjectiveoftheActistoprovidelegalrecognition to e- commerce and to facilitate storage of electronic records with the Government.

TheActprovidesvariousdefinitionsandinstancesofcybercrimes,prescribingthepunishmentforthosecrimesandalsoprovideslawsfortrialofcyberlaw cases in and out of the country.

Sec1oftheITActstatesthat,thisActextendstothewholeofIndiaand,unlessotherwiseprovided,itshallalsoapplytoanyoffenceorcontravention committed outside India by any person.

Sec75oftheITActdealswiththeprovisionsoftheacttoapplyforoffencesorcontraventioncommittedoutsideIndia,irrespectiveofhisnationality,andshallapplytoanoffenceorcontraventioncommittedoutsideIndiabyanypersoniftheactorconductconstitutingtheoffenceorcontravention involves a computer, computer system or computer network located in India.

Sec46oftheITActgivespowertoadjudicateincaseofcontraventionofanyprovisioninthisActandalsoappointsanAdjudicatingOfficerwho is vested with th powers of Civil Courts and are conferred on the Cyber Appellate Tribunal.

AsmuchastheInformationTechnologyAct2000seemsinclusive,itstilldoesposeambiguityinjurisdictionwhentheoffencehasbeencommitted outside of I dia or by a non-citizen, while also following the principle of **Lex Fori**, meaning the law of the country. [10]

ApartofITAct 2000,there areotherrelevantlegislationunderIndianlawsthatgives the authorityto IndiaCourtstoadjudicate themattersrelated to cyber-crimes such as:

Sec3and4ofIndianPenalCode,1882thatdealswithextraterritorialjurisdictionofIndiancourts.

Section188oftheCodeofCriminalProcedure,1973providesthatevenifacitizenofIndiaoutsidethecountrycommitstheoffence,thesameissubject to the jurisdiction of courts in India.

AndSection178dealswiththecrimeorpartofitcommittedinIndiaandSection179dealswiththeconsequencesofcrimeinIndianTerritory.

CYBERSPACE

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintainedbythe worldwide distribution of information and communication technology devices and networks.

With thebenefitscarriedby thetechnological advancements, the cyberspacetodayhasbecomea common pool used by citizens,businesses,criticalinformation infrastructure, militaryand governmentsin a fashion that makes it hard toinduceclear boundaries among thesedifferentgroups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks anddevicesconnected to it.

REGULATIONS

Therearefivepredominantlawstocoverwhenitcomestocybersecurity:

InformationTechnologyAct,2000TheIndiancyberlawsaregovernedbytheInformation TechnologyAct,penneddownbackin2000.Theprincipalimpetus ofthis Act is to offer reliablelegal inclusivenessto eCommerce, facilitatingregistration ofreal-time records with theGovernment.

Butwiththecyberattackersgettingsneakier,toppedbythehumantendencytomisusetechnology,aseriesofamendmentsfollowed.

TheITA,enactedbytheParliamentofIndia,highlightsthegrievouspunishmentsandpenaltiessafeguarding the e-governance,e-banking,ande-commerce sectors. Now, the scope ofITA has been enhanced to encompass all the latest communication devices.

TheITActisthesalientone,guidingtheentireIndianlegislationtogoverncybercrimesrigorously:

Section 43 - Applicable to people who damage the computer systems without permission fromthe owner. The owner can fullyclaimcompensation for the entire damage in such cases.

Section66-Applicableincaseapersonisfoundtodishonestlyorfraudulentlycommittinganyactreferredtoinsection43.Theimprisonmentterm insuch instances can mount up to three years or a fine ofup to Rs. 5 lakh.

Section66B-Incorporatesthepunishmentsforfraudulentlyreceivingstolencommunicationdevicesorcomputers,whichconfirmsaprobablethreeyearsimprisonment. Thistermcanalsobe topped by Rs. 1 lakh fine, depending upon the severity.

Section66C -Thissectionscrutinizestheidentitytheftsrelatedtoimposter digitalsignatures,hackingpasswords,or other distinctiveidentificationfeatures. If proven guilty, imprisonmentof three years might also be backed by Rs.1 lakh fine.

Section66D-Thissectionwasinsertedon-demand,focusingonpunishingcheatersdoingimpersonationusingcomputerresources.

IndianPenalCode(IPC)1980

IdentitytheftsandassociatedcyberfraudsareembodiedintheIndianPenalCode(IPC),1860

-

invokedalongwiththeInformationTechnologyActof2000.TheprimaryrelevantsectionoftheIPCco vers cyber frauds:

Forgery(Section464)

Forgerypre-

plannedforcheating(Section468)Falsedocumentation(Section465)Presentingaforgeddocumentasgenuine(Section471)Reputationdamage(Section4

69)

CompaniesActof2013

ThecorporatestakeholdersrefertotheCompaniesActof2013asthelegalobligationnecessaryfortherefinementofdailyoperations.Thedirectives ofthis Act cements all therequired techno-legal compliances, putting the less compliant companies in a legal fix.

TheCompaniesAct2013vestedpowersinthehandsoftheSFIO(SeriousFraudsInvestigationOffice)toprosecuteIndiancompaniesandtheirdirectors.Also , post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even moreproactive andstern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, andcybersecuritydiligence.TheCompanies(ManagementandAdministration)Rules,2014prescribesstrictguidelinesconfirmingthecybersecurityobligationsand responsibilities upon the company directors and leaders.

NISTCompliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers aharmonizedapproach to cybersecurity as the most reliable globalcertifying body.

NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-relatedrisksresponsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reductionofcybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs Determining the most important activitiesandcriticaloperations-tofocusonsecuringthemDemonstratesthetrust-worthinessoforganizationswhosecurecriticalassetsHelpstoprioritizeinvestments to maximize the cybersecurity ROI Addresses regulatory andcontractual obligations Supports the wider information securityprogram By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurityriskmanagementbecomessimplified.Italsomakescommunicationeasier.

Final Thoughts As human dependence on technology intensifies, cyber laws in India and acrossthe globe need constant up-gradationandrefinements. The pandemic has also pushed much ofthe workforce into a remote working module increasing the need for appsecurity.Lawmakershaveto go theextra mileto stay ahead of theimpostors, in order to block them attheir advent.

Cybercrimescanbecontrolledbutitneedscollaborativeeffortsofthelawmakers,theInternetorNetworkproviders,theintercessorslikebanksandshoppingsites,and,mostimportantly,theusers.Onlytheprudenteffortsofthesestakeholders,ensuringtheirconfinementtothelawofthecyberland - canbring about online safety and resilience.

ROLEOFINTERNATIONALLAWS

Invariouscountries,areasofthecomputingandcommunicationindustriesareregulatedbygovernmentalbodiesλTherearespecificrulesonthe uses towhich computers and computernetworks may be put, in particular there are rules on unauthorized access, dataprivacy andspamming λThere are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes λ Thereare lawsgoverning trade on theInternet, taxation, consumer protection, and advertising λ Thereare laws on censorship versus freedomofexpression,rules on public access to government information, and individual access to information held on them by private bodies λ Somestates limitaccess to the Internet, by law as well as by technical means.

INTERNATIONALLAWFORCYBERCRIME

Cybercrimeis"international"thatthereare‘nocyber-bordersbetweencountries’λThecomplexityintypesandformsofcybercrimeincreasesthedifficulty to fight back ⎝ fighting cybercrime callsforinternational cooperation λ Variousorganizationsand governmentshave alreadymadejoint efforts in establishing global standards of legislation andlaw enforcement both ona regional and onaninternationalscale.

.

.THEINDIANCYBERSPACE

Indiancyberspacewasbornin1975withtheestablishmentofNationalInformaticsCentre(NIC)withanaimtoprovidegovtwithITsolutions.Threenetworks (NWs)weresetupbetween1986and1988toconnectvariousagenciesofgovt.TheseNWswere,INDONETwhichconnectedthe IBM mainframeinstallations that made up India’s computerinfrastructure, NICNET (the NIC NW) a nationwide very smallapertureterminal(VSAT)NWforpublicsectororganisationsaswellastoconnectthecentralgovt withthestategovtsand districtadministrations,thethird NW setup was ERNET (the Education and Research Network), to serve the academic and researchcommunities.

NewInternetPolicyof1998pavedthewayforservicesfrommultipleInternetserviceproviders(ISPs)andgaveboosttotheInternetuserbasegrowfrom1.4 million in 1999 toover150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access throughmobilephones and tablets. Govt is making a determined push to increase broadband.

penetrationfromitspresentlevelofabout6%1.Thetargetforbroadbandis160millionhouseholdsby2016undertheNational BroadbandPlan.

NATIONALCYBERSECURITYPOLICY

National Cyber Security Policy is a policy framework by Department of Electronics andInformation Technology. It aims at protectingthepublic and private infrastructure from cyberattacks. The policy also intends to safeguard "information, such as personal information (ofwebusers), financial and banking information and sovereign data". This was particularly relevant in the wake of US National SecurityAgency(NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguardsagainstit.MinistryofCommunicationsandInformationTechnology(India) defines Cyberspace as a complex environment consistingofinteractions between people, software services supported by worldwide distribution of information and communication technology.

VISION

Tobuildasecureandresilientcyberspaceforcitizens,business,andgovernmentandalsotoprotectanyonefrominterveninginuser'sprivacy.MISSION

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat,reducevulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes,technology,andcooperation.

OBJECTIVE

MinistryofCommunicationsandInformationTechnology(India)defineobjectivesasfollows:

- To create a secure cyber ecosystem in the country, generate adequate trust andconfidence in IT system and transactionsincyberspace and thereby enhance adoption of IT in all sectors of the economy.
- Tocreatean assuranceframeworkforthe designofsecuritypolicies andpromotionandenabling actions for compliance toglobalsecurity standardsand best practices by wayof conformity assessment (Product, process, technology & people).
- TostrengthentheRegulatoryFrameworkforensuringaSECURECYBERSPACEECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats toICTinfrastructure, creating scenarios for response, resolution and crisis management through effective predictive,preventive,protective response and recovery actions.

CYBERSPACE

Definitions,Meaning,FundamentalsandUnderstandingofCyberSpace

Thetermcyberspacehasgarnerednumerousdefinitionsandinterpretationsgivenbybothexpertsandlexicographers.**AccordingtoAdnan(2010),cyberspaceisanunrealworldwhereinformationisconstantlytransmittedthroughorbetweencomputers.**

Ontheotherhand,thecyberspaceaccordingto**pfaffenberger(2000)referstothevirtualspacethatcomputersystemshaveaidedinitscreation.**

Accordingto**ChipMorningstarandF.RandallFarmer**,**cyberspaceisdefinedmorebythesocialinteractionsinvolvedrather than itstechnical implementation.**In their view, the computational mediumincyberspace isan augmentationof thecommunicationchannelbetween real people; the core characteristicof cyberspace is that it offersan environmentthat consists of manyparticipants with theabilitytoaffectandinfluenceeachother.Theyderivethisconceptfromtheobservationthatpeopleseekrichness,complexity,anddepthwithin a virtual world.

Historyoftheword-CyberSpace

ThetermCyberSpacewasintroducedby**WilliamGibson**inhisbook**“Neuromancer”**in1984.Although**Gibson**criticizedthetermbycallingitredolentandmeaningless.Itisstillusedworldwidetodescribefacilitiesorfeaturesthatarelinkedtointernet.

Gibsoninitiallyexplainedthecyber Spaceas***“aconsensualhallucinationexperienceddailybybillionsoflegitimateoperatorsineverynations.”***

Programmedeveloperssuchas**ChipMorningstar**statedthatthecyberspacegaineditspopularityasmediumforsocialinteractionasopposedtoitstechnical execution and implementation.

Thus,unlikemostcomputerjargon,the‘cyberspace’doesn’thaveastandardorobjectivedefinition.Instead,itissimplyusedtodescribesystemsthat extend across a global network of computers.

Cyberspacereferstothevirtualcomputerworld,andmorespecifically,anelectronicmediumthatisusedtofacilitateonlinecommunication.Cyberspacetypicallyinvolvesalargecomputernetworkmadeupofmanyworldwidecomputersubnetworksthatemploy TCP/IPprotocoltoaidincommunication and data exchange activities.

Cyberspaceisaninteractivedomain madeupof digitalnetworks thatisusedtostore,modifyandcommunicateinformation.Itincludestheinternet,butalso the otherinformation,systems that supportourcompanies,infrastructure andservices.

Cyberspacecanbedividedintoamulti-layermodel:

1. **Physicalfoundations**:suchaslandandsubmarinecables,andsatellitesthatprovidecommunicationpathways,alongwithroutersthatdirectinformationtoitsdestination.

2. **Logicalbuildingblocks**:includingsoftwaresuchassmartphoneapps,operatingsystems,orwebbrowsers,whichallowthephysicalfoundationstofunction and communicate.

3. **Information:**thattransitscyberspace,suchassocialmediaposts,texts,financialtransfersorvideodownloads.Beforeandaftertransit,thisinformationisoften storedon(andmodifiedby)computersandmobiledevices,orpublicorprivatecloudstorageservices.

4. **People**:thatmanipulateinformation,communicate,anddesignthephysicalandlogicalcomponentsofcyberspace.

Collectively these tangible and intangible layers comprise cyberspace, which we are increasingly dependent on for essential components of dailylife.Adependableandstablecyberspace is necessaryfor the smoothfunctioning of criticalinfrastructure sectorssuchasenergy,transport,food,health andfinance.Asdependenceincreases,sodothecostsofdisruption—whetheraccidentalorintentional—aswellaspossibilitiesformisuseandabuse.

Insidetheinternetisyetanothercircle—theweb,orthepagesthatcanbeaccessedusingawebbrowsersuchasFirefox,ChromeorSafari.Theinternetandwebareoftenusedinterchangeably,butinfacttheyaredifferentandoneofthemsitsinsidetheother.
Althoughthischapter(andmostpopularcommentary)talksaboutcyber security,whatisreally meant is security of the internet, wherethe vast majority ofglobal communication takes place.

The fourlayers of cyberspacedescribed above (**physical, logical, information, andpeople**)havethreeprimarycharacteristics—**connectivity, speedandstorage.**Thesecharacteristicsenableboththepositiveandnegativeaspectsofthedigitalenvironmentandshouldbeunderstoodinordertoplacecyberspaceincontext.Thisisalsohowreaderscanbegintounderstandcybersecurity—byexaminingthebasiclayersofcyberspaceandtheircharacteristicsandanalysingwhatthismeansforthesafetyandstabilityofthemoderndigitalworld.

Connectivity

Nearly40 percent ofthe world’s populationis connectedto theinternet, through PCs,laptops,tablets andmobilephones. In addition,there are billionsofotherconnected ‘things’suchassensorsembeddedincars,factories,buildings,airplanes,TVsandtoasters.Thisrapidlyincreasingconnectivityproducesvalueand benefitsthataremorethanthesumoftheindividualparts.Thisisknownasapositive‘networkeffect’—asmoredevicesareconnected,moreinformationisgeneratedandshared,andthevalueofthenetworkincreasesforeveryone.

SpeedWhydoescyberspaceseemtochangesoquickly,presentingopportunitiesandchallengesatgreaterspeedthanweareaccustomedtointhephysicalworld?Thereareanumberofreasonsforthischange,andtheyarescatteredthroughoutthetwentiethcentury.

includetheinventionsofthesemiconductorandtransistor.Steadyadvancesintechnology led Gordon Moore (co-founder ofIntel)tostatehisbeliefthatengineerswouldbeabletodoublethenumberoftransistorsonacomputerchipeverytwoyears. This observation,knownasMoore’sLaw,wasmadein1975andhasheldtrueforthepastfourdecades.Itmeansthatthespeed—processing power—of computer chips increases steadily, making laptopsmorepowerful,turningsmartphonesintohandheldcomputers,andallowingGooglesearchestobecompletedever-faster.

Storage

Greater connectivity and speed are nice, but they mean little without storage. What good isan email, text, spreadsheet ordocumentifitcanbesentandreceived,butnotstoredand retrieved? Storage capacity has come close to matching Moore’s Law(namely,doublingroughlyeverytwoyears)asharddriveshavemovedfromgigabytestoterabytesandcontinuetogrow.

Storageinvolvesnotonlycapacity,butalsoperformance,whichistheinput/outputspeedofastoragedevice.Performancehas increaseddramatically withthetransition,over thepastdecade, from traditional harddrives with spinning discs to solid state harddrivesthathavenomovingparts—thesamestorageinsmartphonesandflashdrives.Storageallowsinternetuserstodownloadandretain music, videos,pictures.

Cyberspace'scorefeatureisaninteractiveandvirtualenvironment forabroadrangeofparticipants.In

the common IT lexicon, anysystem that has a significant user base or even a well-designedinterfacecanbethoughttobe“cyberspace.”

Cyber space is the virtual computer world that could be an object that is floating around a computer network or system.Cyberspacehasnowextendedtotheglobalcomputernetwork as well. A better understanding of cyber space can bedeveloped byfinding the answer of following questions:

1) WhatExactlyIsCyberspace?

Let us delve deep into understanding what Cyber space actually is. Cyberspace is where users are allowed to share variedinformation,swapideasandinteract,playgames,andengageinvarioussocialforums.Theycanconductbusinesshereandindulgeinvariousactivities.Itisanyfeaturethatislinkedontheinternet.Everykindofavirtualinterfacethatcreatessomeformofdigital reality is cyberspace. Global content can be used for various purposes thatcouldincludeentertainmentandcommerce.Itishowhumansocietymakesitiswhatdefines cyberspace. So what is cyberspace? Cyberspace exists when thestakeholdersholdvirtualmeetings.Theuseofsmartphonesbringsthesensethatthereisgrowthincyberspace.

Also,massivegamingplayersonlineisanexampleofcyberspace.Herepeopledonotsitfacetofacebutgetconnectedthroughthedigitalworld.

Cyberspacealsocomesintothepicturewhenthereislanguagetranslationthatoccursautomaticallyintheblinkofaneye.

Inanutshell,whenyoudefinecyberspace,cyberspaceiseverythingthatusestheinternet.Itisevolvingandalsopromisestogetmorediverseasyears come by.

1) WhatistheUseofCyberspace?

Nowletustalkaboutwhatusecyberspacehasforus.Weliveinaninterneteraandthe indispensabilityoftheinternetissomethingthatwecannotdenyabout.Theexpandingcomputernetwork,technologies,andtheinternethaveevolvedinto what isknownascyberspace.Itisavirtualenvironmentwherethereiscommunicationbetweencomputernetworks.

Cyberspacebringsinmanyuses.Itletsyoudoeverythingpossiblethroughtheinternet.Beiteducation,military,finance,oreveneducationtodayeverythingisconnectedtowhatisknownascyberspace.Thereisnotasinglesphereinourlifethatisnotconnected to social media.

Theinternethasmadeitefficienttostoreandtohandledata.Ithasmademan’slife organizedandmoresystematic.Beitfor e-bankingorbookingticketsoreventoworkonline, cyberspace iseverywhere.

2) WorkingofCyberSpace

Cyberspaceallowsuserstoshareinformation,interact,swapideas,playgames,engageindiscussionsorsocialforums,conductbusinessand createintuitivemedia,amongmanyotheractivities.Weknowthatcyberspaceissomethingwithoutwhich life cannot be imagined today. So how does cyberspace function? Be it from up in space or from under the water,understandhowtheinternetmakesitpossibletotransferinformation.Itseemsprettystraightforwardtogetonline.However,thereismuch more than what occurs backstage.

Hidden below the sea level and above the surface of the earth,there are complex and largecables as wellasnetworking satellitesthat let you stream your favourite movie and use themaps to navigate to your preferred location. There are many physicalinstallations that let you be connected wirelessly.

Privatehands mostly develop and maintain cyberspace infrastructure.We are allonline butnointernationalorcentralizedauthoritycontainswhat occurs on the internet or how cyberspaceismanagedandstructured.Therearesubmarinecablesthattransmitthedatamakinguseoffiberoptictechnology.Thesesubmarinecablesarethemajorcarriersofdataandtheytransmitlotsofdata cheaply andquickly.

3) IsCyberspaceTheSameAsTheInternet?

Cyberspaceandtheinternethavebeencapableofcreatingavirtualworldforculturalaswellasforvarioussocialpractices. With virtual cyberspace reality, it is now possible to see, communicate, and represent information. Thecyberspaceinternetisavirtualworldofcomputersthatfacilitatescommunicationonline.Itisaworldwhereinformation getstransmitted throughthe internet. **Cyberspaceinternetishoweverdifferentfrom theinternet.** Theinternet isa globalnetwork of computers that offers information and facilitates communication through the networks that areinterconnected.Thisitdoesby using standardized communication protocols.

Thecyberspace internet on theother handis the virtual worldof computers whichis theworld over avirtualcomputernetworkenvironment.

To understandthecyberspacemeaningandits differences clearlyitcanbesaidthattheinternetis asetof networks ofcomputers that make use of the internet protocol to communicate.Thisistheinternet.Cyberspaceisaninformationworldthroughtheinternet.

4. Isthewebnottheinternet?

Whencybersecurityismentioned,manypeopletendtothinkofthesecurityoftheirdevices,homeorworkcomputers,orthe websites they visit on a daily basis. But cyber- space is much larger than thisand includes the sum of global digitalnetworks.Itincludesalldigitalcommunicationsincludingobscureandlegacycommunicationprotocolsorisolatednetworks (forexample,nuclearweaponssilos)thatarenotaccessiblethroughtheinternet.Theinternet(theIP—orInternetProtocol—network)isaslightlysmallercirclethatincludesthemostpopularandwidelyusedformsofcommunication.Authorandjournalist**JohnNaught on**providesausefulanalogytodescribethedifferencebetweentheinternetandtheweb:
"Think of the internet as thetracks and signalling,the infrastructure on which everythingruns. Inarailway network,different kindsoftrafficrunontheinfrastructure—high-speedexpresstrains,slowstoppingtrains,commutertrains,freighttrainsand(sometimes)specialist maintenance and repair trains".

Ontheinternet,webpagesareonlyoneofthemanykindsoftrafficthatrunonitsvirtualtracks.Othertypesoftrafficincludemusicfilesbeing exchangedviapeer-to-peernetworking,orfromtheiTunesstore;moviefilestravellingviaBitTorrent;softwareupdates;email;instantmessages;phoneconversationsviaSkypeandother VoIP(internettelephony) services;streaming video andaudio;andother stuff tooarcane tomention.

Jurisprudenceofcyberlawsinindia Introduction:

Jurisprudencecanbedefinedas thescienceandphilosophyortheoryof thelaw. Applyingjurisprudencetocyberlaw gives rise to the legal study that concentrateson the logical structure, the meaningsand usesof its concepts, and theformal termsand modes of operation of cyber law. Cyberlaw is a very recent concept and if compared with other older branches of the law, is a little structuredstudy.

The term cyberspace was originally coined by a science fiction writer William Gibson to depict data matrices existing in a dark distantfuturewhichmeanstheinformationspacesmadebythetechnologyofdigitalnetworkedcomputersystemsthatultimately connectwiththemotherofallnetworksthatistheInternet.Withtheadventoftheinternetandtechnology,cyberspacealongwithanumberof crimesrelatedtothesameemergedandexpanded.Asweenterthecyberage,thelawonallfrontsisstrugglingtokeeppace withtechnological advances incyberspace.Whilethere isa prosperous discussionof the nature ofcyber lawand its challenges, still a

fundamental body ofscholarlycontributions tothe discussionis lacking. The outgrowth of cyber jurisprudence around the world has promoted the emergence of newer dimensions in Law. The focus is on the practical aspect of cybercrime with the initial attempt to extend the known physical society concepts to the virtual space rather than the theory, philosophy, and science of cyberlaw generally. Hence in due course, we need to develop separateCyber Jurisprudence to deal with future disputes.

Themodern jurists have been cautious to endow with the rationale pedestal of jurisprudence tothis ruling and nowascertained utmost exact definition of cyber jurisprudence as this describes the principles of legal issues, which exclusively regulates the cyberspace and internet can be termed as cyber jurisprudence with a virtual approach[1]

JurisprudentialAspectsofCyberLaws

Cyber jurisprudence givesananalysis oftheland withland and noborder, differentfrom the physicalworld, theymay be virtual from origin and nature. This covers the virtual world with virtual rules and policies, along with the virtual subject matter,virtual contracts, virtual disputes, virtual property, virtual possession, and virtual court.

The existence of anitem in thecontext of a virtual world,such as an e-mail account or an onlinegame, is alsoaform of virtual property. It emphasizes thecompositeidea of cyber jurisdiction, cyber court's venuein the cyberspace, and recognize uniform cyberrulesandpoliciesattheinternationallevel.Framingrulesandlawstocovereveryaspectwillbeanarduoustasksincethe cyber world has no boundaries.

However,abalancehastobemaintainedandlawsbeevolvedinordertokeepacheckoncybercrimes.[2]Wheneveraconflict isencounteredinimplementingexistinglawsoftherealspacetoCyberSpace,thelawsoftherealspacehaveprevailed,overtime thistendencyislikelytodevelopintoaprincipleof"PrimacyofMetaSpace"andbecomethebedrockofJurisprudence.[3]However,the principlefails when two laws of the real space itself come intoconflict in the Cyber Space.

ApplyingJurisprudencetoCyberhasthreepossibleoutcomes:

- ***There exists no relationship between jurisprudence in general and cyber law in particular:*** Here we return to The Law of the Horse. Everything existing at present is sufficient and determining outcomes with a special view to cyber science is unnecessary. No special philosophy or theory of law is necessary to treat events occurring in cyberspace.
- ***Such a relationship exists but it does not require a new jurisprudence to understand it:*** Here thecyber law is recognized as a special area of the law and acknowledges that current jurisprudential thinking is adequate to apply existing theory to its study and analysis.

- ***A new jurisprudence and a new view of cyberlaw are necessary:*** This concludes that cyber law is aspecial and uniquefield of thelaw and it requires a special and unique philosophical and theoretical treatment of its own.

Eventually, the question of whether is it feasible and necessary to create an extensible jurisprudential approach to law that acknowledgesandkeepspacewithcybersciencewithoutbeingasetofrestrictiveandinhibitoryguidelinesthatarebothconfining and resistant to change should be taken into consideration.

EvolutionofCyberLaw

CyberCrimes

InIndia,CyberCrimeisnotdirectlydefinedbyeitherITAct,2000,ITAmendmentAct,2008,oranyOtherLegislation.However, theOffenceorCrimehasbeendefinedbyTheIndianPenalCode1860:asanyOffenceorCrimeinwhichacomputerisusedisaCyber Crime. Cyber or Computer Crimeswere defined asunethical, unauthorized, and illegal behavior of Individualsor asGroups relating to the automatic processing and transmission of data use of Computer Systems and Networks.

CyberCrimesaremajorlyclassifiedintofourtypes:

1. ***AgainstIndividuals:***
    1. HarassmentthroughE-Mails/Messages
    2. Cyber-Stalking
    3. PropagationofObsceneMaterialontheInternet
    4. Defamation
    5. Hacking/Cracking
    6. IndecentExposure.
2. ***AgainstPropertyofanIndividual:***
    1. ComputerVandalism
    2. TransmittingVirus
    3. InternetIntrusion
    4. UnauthorizedControloverComputerSystem
    5. Hacking/Cracking
3. ***AgainstOrganization:***
    1. Hacking&Cracking
    2. CustodyofUnauthorizedInformation
    3. usingCyberTerrorisminoppositiontotheGovernmentOrganization
    4. DistributionofPiratedSoftware
4. ***AgainstSocietyatlarge:***
    1. Pornography(especiallyChildPornography)
    2. SpoiltheYouththroughIndecentExposure
    3. Trafficking

In India, the Cyber Crimes have grown from 9,622 and 11,592 to 12,317 during 2014, 2015, and 2016 respectively.[4]The National Crime Records Bureau (NCRB) and Indian Computer Emergency Report Team (CERT-In) had reported that approximately 80 phishing incidents affecting 20 Financial Organization, 13 incidents affecting various Automated Teller Machines, Point of Sales systems, and Unified Payments Interface (UPI).

Legislations

The principal source of cyber law in India is the Information Technology Act, 2000 (IT Act) with the primary purpose to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. This Act penalizes various cyber crimes and provides stringent punishments including imprisonment terms upto 10 years and compensation upto Rs 1 crore. Some of the major Acts got amended after the enactment of ITA:

1. ***TheIndianPenalCode,1860:***Theword'electronic'wasadded,therebytreatingtheelectronicrecordsanddocuments onaparwithphysicalrecordsanddocuments.TheSectionsdealingwithfalseentryinarecordorfalsedocument[5]havesince been amended as 'electronic record and electronic document' to bring it within the ambit of IPC.
   Now, electronic records and electronic documents have been treated on par with physical records and documents duringthecommissionofactsofforgeryorfalsificationofphysicalrecordsinacrime.
   Theinvestigatingagenciesstartedfilingthecasesandcharge-sheetsquotingtherelevantsectionsfromIPCreadwith the ITA/ITAA in like offense in order to ensure that the evidence and/or punishment can be brought under its scope and be proved under either of these or both the legislation.
2. ***The Indian Evidence Act 1872:***Before enactment of ITA, all pieces of evidencein acourt werein the physical form onlyandnowtheelectronicrecordsanddocumentswererecognizedasthedefinitionpartofIndianEvidenceActwasamended as "all documents including electronic records". Words like 'digital signature', 'electronic form', 'secure electronic record''information' asused in the ITA were also insertedafterthisamendmenttobeapartoftheevidentiaryimportanceundertheAct. TheidentificationandrecognitionofadmissibilityofelectronicrecordsasevidenceasenshrinedinSection65BoftheAct was seen as a significant amendment.
3. ***TheBankers'BooksEvidence(BBE)Act1891:*** Previouslybankswererequiredtoproducetheoriginalledger,other physical registers, and document during evidence before a Court but now the definitions part of the BBEAct stood amendedas:"bankers'books'includeledgers,day-books,cashbooks,account-booksandallotherbooksusedinthe ordinarybusinessofabankwhetherkeptinthewrittenformorasprintoutsofdatastoredinafloppy,disc,tapeorany other form of electromagnetic data storage device"[6].ThisamendmentintheprovisionsinBankersBooksEvidenceActrecognizedtheprintoutfromaco mputersystemandanotherelectronicdocumentasavaliddocumentduringevidence,provided,suchprint-outor electronic document is accompanied by a certificate by a person-in-charge of computer system.

JurisdictionalCyberIssues

TheoriesofJurisdiction

As far a cyber law is concerned, the jurisdiction encompasses several discrete concepts, including jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce.[7]The prescribing jurisdiction is a sovereign entity's authority to make applicablelawstotheactivities,relations,orstatusofpersons,ortheinterestsofpersonsinthingsbylegislation,byadministrativeruleorby determination of a court, by executive act or order and jurisdiction to adjudicate is a sovereign entity's authority to subjectpersonsorentitiestotheprocess ofitscourtsoradministrativetribunalstodeterminewhetherprescriptivelawhasbeen violated.[8]There are various theories of jurisdiction:

1. **TerritorialityTheory:**Itmeansthatasovereignstatehastheauthoritytojudgecriminalactsthathavebeencommitted in its territory. The place where the crime is committed has to be established for this to apply.
2. **NationalityTheory:** AlsoknownasPersonalitytheory,recognizesthatasovereignstatecanadoptcriminallawsthat govern theconduct of nationals while outsideof itsborders. Thisprincipleeffectivelymakes it acrimefor its nationalsto engage inconductthat is not illegal inthe placewhere the conduct is performed. This theory isfurther dealt within two ways:
    1. **Active Nationality Theory:** This theory recognizes that a state may exercise criminal jurisdiction over its nationals based on their active nationality and can prosecute and punish its sovereign nationals for committing a crime outside its territory.
    2. **PassiveNationalityTheory:**Thistheoryprovidesforasovereigntoadoptcriminallawsthatapplytoforeign nationalscommittingcrimesagainstthesovereign'snationalswhilethesovereign'snationalsareoutsideofthe sovereign's territory.
3. **ProtectionTheory:**Thistheoryprovidesforasovereigntoadoptastatutethatcriminalizesconductthatoccursoutside of its borders and when that conduct affects the sovereign itself. The sovereign can make it a crime to engage in an actthatobstructsthefunctionofgovernmentorthreatensitssecurityasastatewithoutheedtowhereorbywhomthe act is committed.
4. **UniversalityTheory:**Thistheoryprovidesforasovereigntoadoptcriminallaws applicabletotheconductperformedbyany person anywhere in the world when such conduct is recognized by nations as being of universal concern.
5. **Derived Jurisdiction Theory:** This theory cannot betreated as an independent basisfor jurisdiction.If thestate that has jurisdiction, so determines orauthorizes a state that has nojurisdiction over certain acts according toits national laws or case law and embodied principles then it may assume jurisdiction. This can be carried out in the form of a formal request or based on an international treaty.

PrinciplesofJurisdiction

i. **TerritorialityPrinciple:**
    - ifoneoftheactsconstitutinganelementoftheoffensehasbeencommittedintheterritorythentheoffenseissaidto be committed within the territory of a state
    - iftheeffectsoftheoffensebecamemanifestthere.

ii. **TheFlagPrinciple:**Thisprincipleisconsideredtobeavariantoftheterritorialityprincipleanditappliesifthe cybercrime is committed on aship or aircraft that is beyond theterritory of the Flag party, thestate of registry will be the one exercising jurisdiction over the offense.

iii. **NationalityPrinciple:** It applies the active nationality principle. It gives an obligationto nationals of astate tocomply with the domestic law even when they are outsideits territory. This prevents nationals of astatetotravel to aforeign state to commit a cybercrime and return without the risk of being prosecuted.

DoctrinalApproach:

Meaninganddefinition

Dr S.R. Myneni has defined, "A doctrinal research means a research that has been carried out on a legal proposition or propositions by way of analyzing the existing statutory provisions and cases by applying the reasoning power." (Tiwary 2020)

Doctrinalresearchhastherootword"doctrine"whichmeansaprincipleorabasicgoverningtenet.Thatmeans, thelegaldoctrinewouldincludelegalprinciplesandtenetsthatwouldgovernthelegalworld.Therefore,itimplies that doctrinallegalresearchwouldinvolvediggingdeeperintothelegalprinciplesandconceptsfromvarious sources like cases, precedents, statutes and others; to analyze them and reach valid conclusions.

The focal point of doctrinal research is answering the question "What is law?". It is library-based research, i.e. we try to find out definite answers to legal questions through a thorough investigation from the law books, statutes, legislation, commentaries and other legal documents. All of these sources fall under the category of "Secondary Sources". As stated earlier, it is theoretical research that does not involve any kind of experimentation or fieldwork.

Here, we are basically checking the validityof existing laws in light of a changing society. It begins with one or morelegalpropositionstakenasastartingpointandtheentireresearchisdirectedinfindingthevalidityofthat hypothesis. It simply means reviewing and studying different legal documents and other sources and then deducingacompleteanswertothequestionaskedat thebeginningbythemeansofrationalinterpretationand logicalreasoning.Mostoften,thestartingpointinanyresearchisdoctrinal,i.e.library-basedandthenwemoveforwardto other methodologies once our base is set by doctrinal research. This is the reason that doctrinal research is very famous among students and academicians.

History

Therootsofdoctrinalresearchcanbetracedtothepositivistortheanalyticalschooloflawwhichwasobjective andvalue-free.Itismoreepistemologically oriented anddoesnotconcernitself withpeopleor society. Though the law itself is normative, doctrinal research does not studyit in a normativesense. It does not takeinto considerationthe humanaspectsoflawandhowitaffectspeopleinsociety.Inthistypeofresearch,wejust concernourselveswithexistinglawsinthepresentstateastheyare.Itsemergencecanbetracedparalleltothe riseofcommonlawinthenineteenthandtwentiethcentury.Commonlawhasbeendevelopedbytheeffortsofjuristsand theCourt’sdecisions.Thedoctrineofprecedentsalsodevelopedaroundthesametime.Allofthese developments are linked to doctrinal research as without it the other parallel developments would have been incomplete.Itiswhenjudgesandattorneysinvestigatedlawsfromvariousabove-mentionedsources,thatthey could set the stage for the progress of common law.

Andweallknow,commonlawisthebasisoflegaldevelopmentinseveralothercountries.Atasimilartime,thelawhadentered theacademicfieldinEuropeanddoctrinalresearchpickeduppaceasitbecameapopular tool of academiclegalresearch.(Tiwary2020)This is thereasonwhydoctrinalresearchis alsoknownas traditional research.

Purpose

One of the main purposes of conducting doctrinal research is solving the legal problems of bringing laws. For example,ifthegovernmentdecidestobringumbrellalegislationforallthecrimescommittedagainstwomen,it may initiate doctrinal research by some jurists and experts in the field.

They may have to go through all the existing laws in this field, previous case laws, precedents, international trends, legal commentaries, articles by scholars, dictionaries, encyclopedias, journals, treatises, textbooks and other sources of legal information. Going through this sea of information, they would be able to answer all the questions related to this legislation and will be successful in bringing out comprehensive legislation.

It can be utilized for several other purposes as well like to help lawmakers develop meaningful and effective laws,developfreshlegaldoctrines,aidcourtsinreachingeffectiveandlegallyaccuratejudgments,helplawyers to interpret statutes and prepare their suits, help students in academia to set a base and many others.

Methodology

Themethodologyindoctrinalresearchstartswithsettingapropositionasthestartingpoint.Alegalprovisionin questionor an existing law could be chosen for the purpose. The next step could be to analyze the purpose behind bringing that particular law. For example, for a provision of the constitution, Constituent Assembly Debates could give great insight.

The law then can be studied in greater detail. A course of action must be selected. Alternative courses can be explored. Different models need to be studied and finally, the consequences and approximated effects have to beweighedinordertoaccuratelymakepredictionsaboutthepropositionsetatthebeginning.Inallthesestages,secondary sources talked about in the above paragraphs are utilized.

But one must be very careful in the selection of these sources. Searching for reliable and accurate sources demands time and effort. Useful information must be separated from the chaff as the presence of unreliable informationcouldleadtomisleadingandinaccuratelyskewedresults.Theefficiencyofthismethodalsodepends on the question that is asked in the beginning. Asking the right question is the first step towards concrete research. Setting the right proposition and then relying on the right sources is the key to successful doctrinal research.

Advantagesanddisadvantages

To begin with the advantages, doctrinal research forms the base of legal research in the academic field of law. Law students atthegraduateandpost-graduatelevelsusually ventureintotheworldof legalresearchwiththe helpofdoctrinalmethodology.Thisisthestartingpointforthemwheretheycananalyzesourcesavailablein the library andlogically deduce theirfindings. Thestudents arenotwell equippedat thisparticular stagetoget involved with empiricalresearch and to consider the law inthe contextof society.Itis easier for themto study law “as it is” from secondary sources and it acts as a good starting point.

In addition, it gives the judges and lawyers the flexibility to approach law from different aspects and make its interpretation. It may not be wrong to say that the amorphous mass of the present-day statutory provisions takes concrete shape and form in the great laboratories of the law courts. (Jain 1982) Judges have over time developed law from their deep knowledge and investigation into the field. Law of torts is one great example as it is a “judge-made law”. Therefore, doctrinal research being the traditional methodology has helped in the developmentoflegalresearchbygivingitabase.Ithasbeenaclosecompanionoflawacademicians,students, judges, advocates and jurists.

However,doctrinalresearchhasitsownshortcomingsaswell.Availabilityandchoiceofrightandreliablesources isthebottleneckindoctrinalresearch.Logicaldeductionisalsoanuphilltask.Furthermore,itishighlytheoretical andrestricted.Withouttherightdirection,itmaybecomehighlyobjectiveandtoomechanical.Moreover, itcan befurtherhighlightedthatitstudieslawindividuallyanddoesnotconsideritinthebackdropofsocietywhichis the playground of law. Without studying its normative and practical aspects, it’s like studying law in darkness and seems incomplete.

HierarchyofCourts:

TableofContents

Whatisjudiciary?

According to the"*Rule of law",* all individuals whether they are rich or poor, men or women, from forward or backwardcastearesubjectedtothesamelaw.Judiciaryensuresthe supremacyof lawandtheruleoflaw.The law is interpreted by the judiciary but the judiciary cannot make the law. Judiciary resolves the disputes and ensures justice by applying the laws.

JudicialMeaning

Themeaningofjudicialistomakejudgementsinacourtoflaw.Judicialisrelatedtothelegalsystem.

JudiciaryinIndia

India has a single integrated system of Judiciary in view ofa single Constitution. The judiciary in India acts as thecustodianoftheIndianConstitutionandtheprotectoroftheFundamentalRights.TheIndianJudicialSystem is one of theoldestlegalsystemsoftheWorld.TheIndianlegalsystemwasmajorlyinfluencedbythelocalcustoms andthe religion.The judicialsysteminIndiais integratedand pyramidalinstructure withthe Supreme CourtatthetopandtheHighCourtandtheotherSubordinateCourtsatthelowerlevels.Theadversariallitigation systemisfollowedbytheIndianJudicialSysteminwhichtheimpartialneutralpartyandboththesidespresent argumentsbeforetheCourtoflaw.TheCommonlawsystemwhichisfollowedinEnglandinfluencedtheIndian JudicialSystem.Thelawsweredevelopedbythejudgesthroughthejudgementsdeliveredbycourtsandthese judgementswere followed as precedents. The specific feature of theIndian Judicial System is*"judicial review"*. Thejudicialreviewisthepowergiventothejudiciarytodeterminethevalidityoflaw.Article137oftheIndianConstitutionempowerstheSupremeCourtwiththejudicialreviewthroughwhichitcandeclareanylaw asvoidwhenitisunconstitutionalorinderogationwiththeFundamentalRights.Thepowerofjudicialreviewisgiventothe High Courts also through which it can overrule the decisions of the lower courts.

According toArticle 13 of the Indian Constitution, the laws which are contrary to the Fundamental Rights aredeclared as void by the judiciary.

Our Constitution ensures the Independence of Judiciary which means that the other organs of the Government must not restrain the functioning of the judiciary in such a way that it would not be able to do justice. Other organs of the Government should not interfere with its decision and judges must be able to perform their functions without fear or favour. The Constitution of India had granted rights to citizens to ensure equality and protects them from any partial judgement. The power to resolve disputes and to give judgements is basedon the rules of law, is given to judiciary.

According to the members of the Constituent Assembly, " This is the organization which will safeguard those fundamental rights which have been given to every citizen under the Constitution. Therefore, it must be above all obstruction by the Executive. The Supreme Court is considered as the "***watchdog of democracy****."*

Indeed,theIndependenceoftheJudiciaryisentailednottofavourjudges.Itiscrucialtomaintainthepureness of justice and to acquire the trust of people in the administration of justice.

Article 50 of the Indian Constitutionensures the*separation of powers*of the judiciary from the executive.Our Indian Constitution has granted fundamental rights to people and to sustain these rights the judiciary is made independent by it.

TypesofJudiciary

Therearesomanycountriesandeachoneofthemfollowdifferenttypesofthejudicialsystemandfollowsystem according to their own governance.

The United States of America follow the judicial system in which there is a two-court system. The State Court system and the Federal Court system are the two types of court in the USA. These courts are not totally independentfromeachotherastheyusuallyinteractwitheachother.Themainobjectiveofeveryjudicialsystem is to solve legal issues and to vindicate legal rights.

The Article III court is followed in various countries. The Supreme Court, District Courts and Circuit Courts of AppealarethecourtswhichareincludedinArticleIIICourts.TherearetherspecialcourtsliketheInternational Courts and the Court of Claims are also included in the Article III courts.

Therearesecondtypeofcourtsysteminvariouscountrieswhichmayincludethe BankruptcyCourts,Taxcourts,Magistrate courts, Court of Veterans Appeals and the Court of Military. There are various types of State Court Systems and most of them are composed of the two types of trial courts, Traffic and Family courts which are includedinthetrialcourtshavinglimitedjurisdiction.Thegeneraljurisdictioncourtsarealsotherewhichincludes the intermediateappellatecourts,themaintrivialcourtsandthehigheststatecourtsalso.Incontrasttothe Federal Courts, a large number of the State Court Judges are either elected or appointed not permanently but for a specific number of years.

The Trial Courts of limited jurisdiction manage certain sorts of particular cases. Generally, these courts are located near the courthouse of the country or inside the country and usually presided over by one judge. The Municipal Court, family court and probate court are the few types of trial courts having limited jurisdiction. The TrialCourtsofgeneraljurisdictionaretheprincipaltrialcourtsinthestate'ssystem.TheseCourtshearsthe caseswhicharebeyondthejurisdictionofthetrialcourtsoflimitedjurisdiction.Thesecourtsdealwithbothcivil and criminal cases.In most of the states of the U.S., there are intermediate appellate courts in between thehighest court of the State and the trial courts of general jurisdiction. There are some kinds of highest courts in all the States and these are referred to as the Supreme Courts in some States.

Thecommontraditionlawsystemisfollowedin Englandandthissystemisfollowedinthecolonizedcountriesof England also.

There are several countries and each country has a different organization of courts of law which includes the District Courts, theSupremeCourt, the Magistrate Courts,Regional Labour Courts and National Labour Courts. The Magistrate Courts are considered as the primary trial courts. These courts have jurisdiction to deal with criminal matters. The District Courts are the courts at a middle level and these courts deal with the matters whicharenotunderthesolejurisdictionoftheothercourts.TheSupremeCourthastheauthoritytohearcriminal and civil appeals from the District Courts.

FunctionsofJudiciary

Thejudiciaryplayedaneminentroleinamoderndemocraticstate.Itperformsvariousfunctions,like:

- **Interpretationoflaw**

The foremost function of the judiciary is to interpret the law and use them in a particular case by applying the principlesof customs,statutes andvariousprovisionsoftheConstitution.They gothroughthefactsof thecase andanalysewhatlegalrightsofpartiesinthecaseareaffectedandwhatlawshouldbeappliedinthissituation. When the law is lacking, judiciary applies the principle of justice, equity, and morality.

- **GuardianoftheConstitution**

OurConstitutiongivestherighttoallcitizenstoprotectthemselvesfrominequalityandtheCourtprotectthese rights.ThepowerofjudicialreviewisalsogiventotheSupremeCourtofIndiaanditenjoysthepowertodeclare a law passedbythelegislatureasunconstitutionalifthatlawconflictswiththeConstitution.Itisnotonlythe guardianoftheConstitutionbutitalsomodifiestheConstitutionwiththechangingconditions.Ithasalso expandedtheConstitutionthroughinferenceofitsoriginalprovisions.TheIndianSupremeCourthadalso pronounced some laws as *"ultra vires"* on the *rationale* of *"procedure established by law"*.

- **CustodianofCivilLiberties**

The judiciary protects individual liberty by punishing those who intrude against it. It also safeguards people against tyrannical action of the Government. Article 32which is known as the*"heart and soul of the Indian Constitution"* provides right to the people that they can directly approach the Supreme Court in the caseof the infringementofthefundamentalrights.AwritcanalsobefiledintheHighCourtunderArticle226oftheIndianConstitution to protect these rights.

- **ResolvesthedisputesofjurisdictionbetweentheCentreandStateGovernmentsinFederations**

The Constitution of India establishes a federal structure to the Indian Government, so the powers are divided betweentheCentreandtheStates.ThearechancesthatdisputesmayarisebetweentheCentreandtheState over the jurisdiction. Therefore, the Supreme Court is given the right to decide these disputes.

- **AdvisoryFunction**

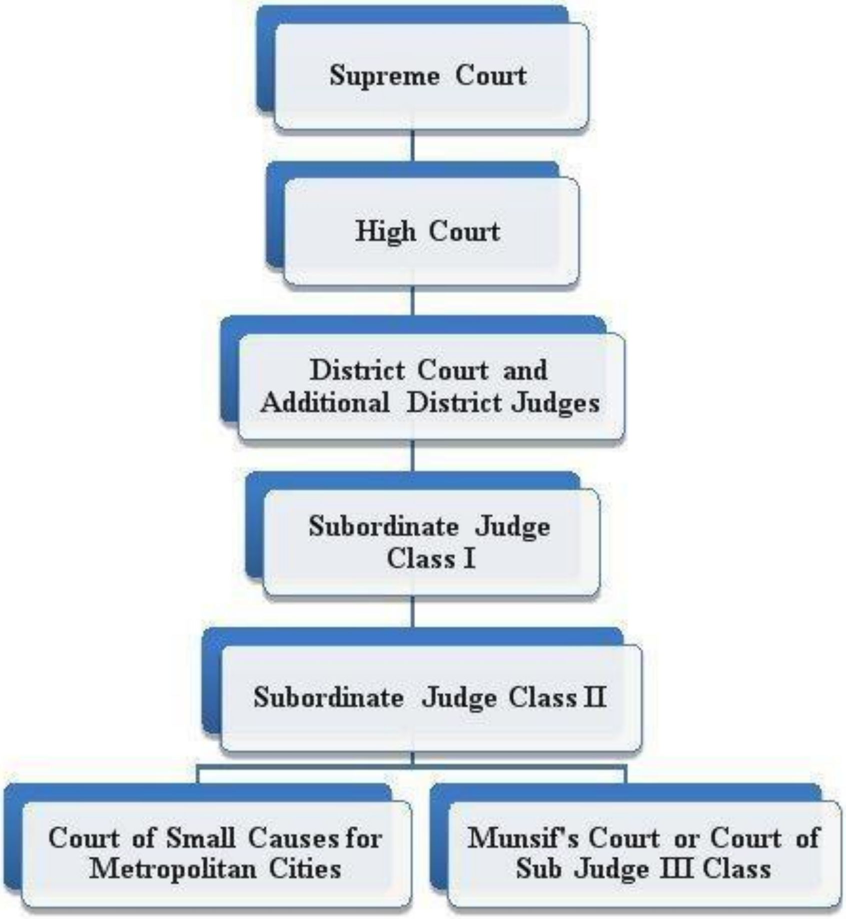
In India, theSupremeCourtacquirestherightfromthe Constitution toadvisethePresidentonthe legalissues. Article 143of the Indian Constitution empowers the Supreme Court with the advisory jurisdiction.

- **AdministrativeFunctions**

TheSupremeCourtandtheHighCourtshavetheauthoritytoappointtheirlocalofficialsandsubordinatestaff.

IndianJudiciaryChart

Hierarchy of courts and their jurisdiction should be properlydefined to deal with the disputes which arise every day in a big country like India. The Supreme Court of India deals with the cases at the National level, the High CourtdealswithcasesattheStatelevelandSubordinatecourts(CivilandCriminal)dealswiththecasesatthe District and Subordinate level.


Supreme Court
High Court
District Court and Additional District Judges
Subordinate Judge Class I
Subordinate Judge Class II
Court of Small Causes for Metropolitan Cities
Munsif's Court or Court of Sub Judge III Class

Imagesource–http://bit.ly/2XfrW9q

TypesofCourtsinIndia–7typesofCourtsinIndia

There are various types of Courts in India, each has different powers depending on the tier and jurisdiction conferred on them. They function according to the set hierarchy of the courts.

SupremeCourt

In our country, the Constitution lays down the foundation of an integrated judiciary having Supreme Court as the highest and final court of appeal. Article 124(1)of the Indian Constitution states that there shall be a Supreme Court of India constituting of a Chief Justice of India. Initially, the Supreme Court of India consists of theChiefJusticeofIndiaandsevenotherjudges.TheParliamentmay,bylaw,increaseordecreasethenumber of judges of the Supreme Court when it is required. Now, the Supreme Court has 31 judges including the Chief JusticeofIndia.InourConstitution,thereisaprovisionofappointmentofjudgesonan *adhoc*basis,whenever itisrequired.Article127(1)oftheIndianConstitutiondealswiththeappointmentof adhocjudges. *Adhoc*isa

Latin term which means "*for this*". It means for aparticular purpose. When a quorumofjudges is not available to continue or hold the sessions of Court then ad hoc judges were appointed. The Chief Justice of India can appointa Highcourtjudgeasan adhoc judgeof theSupremeCourt after consultation with theChief Justiceof the concerned High Court.

ThePresidentofIndiaappointsthejudgesoftheSupremeCourtandthelatercanconsultwiththeChiefJustice ofIndiaandalsowithexistingjudgesoftheSupremeCourtregardingsuchappointment.Incaseofappointment ofthe Chief JusticeofIndia, the President shall consult such judgesoftheSupremeCourt and the High Courts.

1. For apersontobeeligibleasajudgeof theSupremeCourt,he/shemustbeacitizen ofIndia,and should have been for at least five years a judge of a High Court or of two or more such Courts in succession, or
2. shouldhavebeenanexperienceofpracticingasanadvocateofHighCourtforthelasttenyearsor of two or more such courts in succession or
3. shouldintheopinionofthePresidentbeaneminent jurist.

TheSupremeCourtofIndiaisthehighestcourtofappealandisvestedwithvariouspowers,itexercisesoriginal,appellate and advisory jurisdiction.

PowersoftheSupremeCourt

1. The Supreme Court has the power to punish for contempt of Court under Article 129 of the Indian Constitution.
2. The power of Judicial Review is given totheSupremeCourtunder Article32andArticle 136of the Indian Constitution. They have the power to examine the legislative enactments and executive orders whether they are consistent with the provisions of the Constitution or not.
3. Supreme Court is a deciding authority in the election of the President and the Vice President and enquiringauthorityinconductandbehaviourofUnionPublicServiceCommission(UPSC)members.
4. Article134oftheIndianConstitutionempowerstheSupremeCourttowithdrawthecasesfromthe High Court.
5. Article 126of the Indian Constitution states that when the office of the Chief Justice of India is vacantorwhen theChief Justice isbyreasonof absenceorotherwise unable toperformhis duties oftheoffice,thenthePresidentofIndiamayappointajudgeoftheSupremeCourttodispensethe duties of the office.
6. Article 127of the Indian Constitution states that the Chief Justice of India can appoint a judge of HighCourtasan*adhoc*judgeintheSupremeCourtwiththeconsentofthePresidentifatanytime there is a lack of quorum of judges in the Supreme Court.
7. Article128oftheIndianConstitutionstatesthattheChiefJusticeofIndiaatanytimewiththeprior consent of the President and the person to be so appointed can appoint any person who had previously held the office of a judge of the Supreme Court.
8. The Supreme Court has the power of revisory jurisdiction under Article 137of the Indian Constitution through which Supreme Court can review its judgements.

TheSupremeCourtisa***courtofrecord***becauseitsjudgementsareofevidentiaryvalueandcannotbe questioned in any court.

The Procedure to remove the Chief Justice of India and the judges of the Supreme Court is given under Article124(4)oftheConstitutionofIndia.ThePresidentofIndiaappointsthejudgesoftheSupremeCourtofIndia,so the power to remove them from their post is vested upon him. But, according to the Constitution of India, the judiciaryisindependentofthelegislativeandexecutiveorgansoftheGovernment.SothejudgesoftheSupreme Courtcan be removed only on the basis of proven incapacity or misbehaviour.

HighCourt

Article214oftheIndianConstitutionstatesthatthereshallbeaHighCourtforeachState.TheHighCourt consistofoneChiefJusticeandotherjudges.ThePresidentappointstheChiefJusticeoftheHighCourtin consultation with the Chief Justice of India while other judges were appointed by the President in consultation withtheGovernorofthestate,ChiefJusticeoftheHighCourtaswellastheChiefJusticeofIndia.IfintheHigh CourttheofficeoftheChiefJusticefallsvacantduetosomereasonsthenthePresidentcanaskanyoftheJudgetolookafter the duties of the Chief Justice.

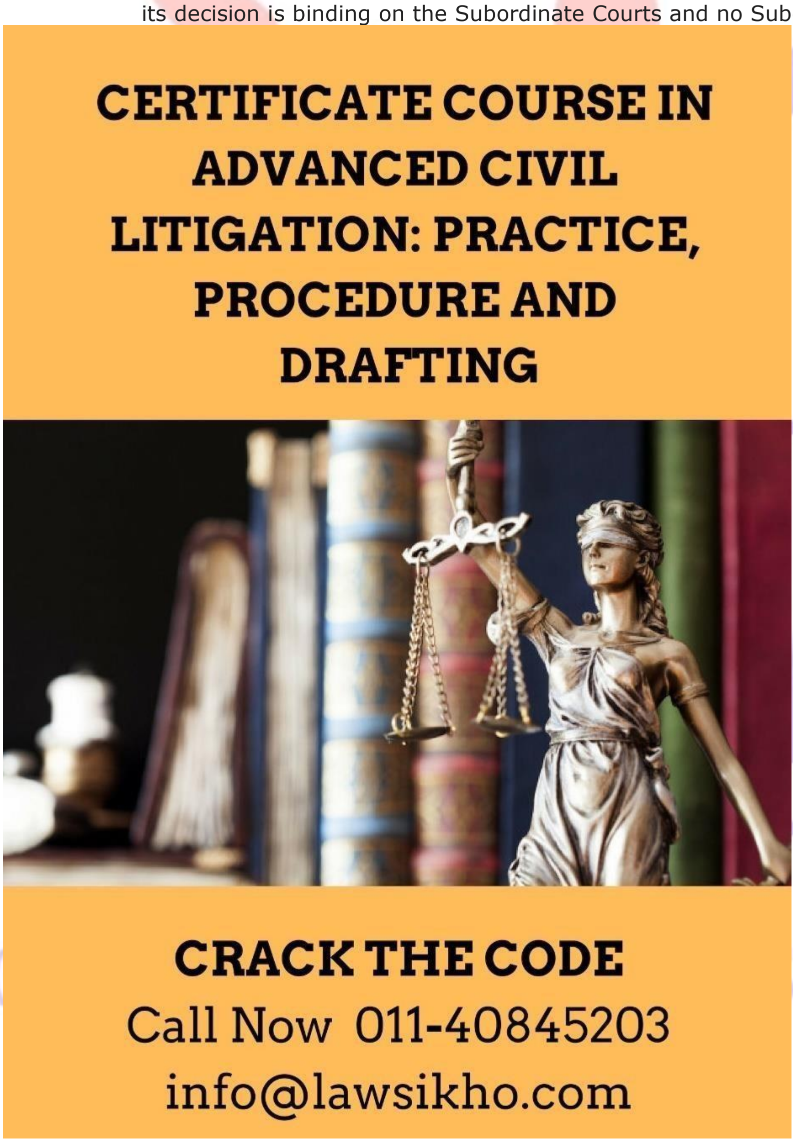
ApersonmaybeappointedastheChiefJusticeoftheHighCourt:

1. IfthepersonisanIndiancitizen,and
2. IfhehadheldthejudicialofficeintheterritoryofIndia,or
3. Atleastanadvocatefor10yearsintheHighCourtortwoormoreHighCourtsinsuccession,and
4. Theageshouldbebelow62years.

Ajudgecanremainintheofficeuntilhehasattainedtheageof62yearsandcanalsoresignbeforetheretirementbygivinga resignationlettertothePresident.HecanalsoberemovedifTheParliamentpassedaresolutionwhichis supportedbythemajorityofthetotalmembershipoftheHouseinwhichthemotionofremovalhasbeen passedandbyamajorityofnotlessthantwo-thirdmembersoftheHousepresentandvotinghasbeen presented before the President, on the grounds of proved misbehaviour or incapacity. He can also vacate the office of the Court when the President appoints him as the judge of the Supreme Court.

PowersoftheHighCourt

1. UnderArticle 226of the Indian Constitution, a person can directly file apetition inthe High Courtin case of infringement of the Fundamental Rights.
2. Election-relatedcasesormarriage/divorcerelatedcasescanbedirectlyfiledintheHighCourt.
3. TheHighCourthasthepowertogivepunishmentforthecontemptoftheCourt.
4. The High Court has the power to review the cases of the lower Court and give its judgement accordingly.
5. TheHighCourtexercisesoriginal,appellate,supervisoryandadministrativejurisdiction.
6. TheHighCourtisacourtofrecordanditsjudgementsareof evidentiaryvaluefortheSubordinate Courtsand its decision is binding on the Subordinate Courts and no Subordinate Courts can challenge them.



CivilCourtsMeaning

Civil courts deal with the cases or offences that are committed against a private individual and not against the StateunlikeincriminalcaseswheretheoffenceiscommittedagainsttheState.Civilwrongsincludetort,breach ofcontractetc.InIndia,thehierarchyofCivilCourtsisbasedontheterritorialandpecuniaryjurisdictionofthecourts.Civil Courtscandealwiththecaseswhichhavebeencommittedwithinitsterritoryandalsowhichiswithinthe pecuniary limits of the court.

The Supreme Court is the highest court of appeal for entertaining civil cases and these cases can not be filed directly in the Supreme Court, the appeal can be filed against the order of the High Court but in case of infringement of the fundamental rights one can directly approach to the Supreme Court.The appeal against the orderoftheDistrictCourtcanbefiledintheHighCourtandthecasesabovethevalueofRs.20lakhscandirectly be filed in the High Court of the State.District Court deals with the cases which lie between the value ofRs. 3 lakh to Rs. 20 lakh. The cases up to Rs. 3 lakhs were entertained by the Civil Judge the junior division and the original cases were entertained by him. Small Causes Courts are the lowest Court of appeal in the hierarchy of Civil Courts and it deals with the cases of value below Rs. 3 lakh. The Civil Courts are governed by the Civil ProcedureCode.TheCivilCourtscanawarddamagesorcompensationtothepartywhoselegalrightshavebeen infringed. Plaintiff and Defendant are the parties to a civil case.

DistrictCourtandAdditionalDistrictCourt

TheStateGovernmentinIndiahasestablishedtheDistrictCourtsineverydistrictbyconsideringthenumberof casesandpopulationinthatdistrict.TheDistrictCourtsofIndiaarepresidedbyadistrictjudgeandthesecourts administerjusticeatadistrictlevel.ThesecourtsareunderadministrativeandjudicialcontroloftheHighCourt of the Statetowhichthatdistrictbelongs.TheDistrictandSessionsJudgeisthehighestCourtineachdistrict. TheGovernor afterconsultationwiththeChiefJusticeof theHighCourtofthatStateappointsthejudgesofthe DistrictCourtandtheeligibilitycriteriatobecomeajudgeofDistrictCourtisatleastsevenyearsofpracticeasan advocate.The DistrictCourt is the highestCivilCourt ina district.Civil and Criminal Courts are two types of Courts in every district. Civil Courts exercise the power of subject matter jurisdiction, territorial Jurisdiction, pecuniary jurisdiction and appellate jurisdiction.

PowersoftheDistrictCourt

1. TheDistrictCourthearscriminalcases,domesticrelatedcasesandcivilcases.
2. The District judgein caseof criminal caseshasthepower togiveanypunishment including capital punishment.
3. TheChief JudicialMagistratecandealwiththecaseswhicharepunishablewithimprisonmentfor a term up to seven years.

When the District Court exercises its jurisdiction in criminal cases under the Code of Criminal Procedure, 1973 (CrPC), it is referred as sessions court. The Court is presided by a judge who is appointed by theHigh Court of that particular State. Additional Sessions Judges and Assistant Sessions Judges in this Court can also be appointed by the High Court of that State. Additional Sessions Judges can be appointed in POCSO cases, electricity cases, NDPS, FTC etc. The appeal can be filed in the High Court against the decision of the District Court.

CourtofCivilJudge(SeniorDivision)

The Court of Civil Judge of Senior Division comes at the middle of the hierarchy on the civil side. Civil Judge or Senior Division has the authority to try civil cases of any value. There are many additional courts of Additional CivilJudge(seniordivision).Theseadditionalcourtshavethesamejurisdictionasexercisedbytheprincipalcourt of Civil Judge or Senior Division. A Senior Division or Civil Judge exercises pecuniary jurisdiction without any limit.

CourtofCivilJudge(JuniorDivision)

TheCourtofCivilJudgeofJuniorDivisionisatthelowestlevelindecidingcivilcases.Ithasthepowertoimpose anysentenceinaccordancewiththelawanditcanprovidecapitalpunishmentalso.CivilJudgeofJuniorDivision can extend its jurisdiction in all the original suits and proceedings.

EligibilitytobecomeCivilJudgeofJuniorDivision:

- AnapplicantmusthavedoneLL.B(BachelorofLaws)/LL.M.(MasterofLaws)with55%from anyuniversity which was recognized by the State Government/Central Government.

- Agelimitis21-35yearsandrelaxationinageisprovidedtoreservedcandidates.

Courtofsmallcausesformetropolitancities

Under the Presidency Small Cause Courts Act, 1882, the court of small causes for metropolitan cities were established in India. This Act empowered the State Government that it can establish a Court of Small Causes anywhere within its territory. These courts have the authority to decide small value civil cases only.

MunsiffcourtorcourtofsubjudgeIIIclass

Munsiff court is the lowest court of appeal for civil cases in the district. It has the authority to try the offence under certain pecuniary limits. Munsiff Magistrate/ Judicial Collector have control over these courts.

The territorial jurisdictionof the District Munsiff Court wasprescribedby the State Government. The judge and presiding officer of the District are Munsiff Magistrate who keep a charge on all the tax inspectors.

CriminalCourtMeaning

Criminalwrongisawrongagainstthewholesocietynotonlyagainstthevictim.CriminalCourtsdealwithcriminal matters which are considered as a crime against the State.

The Supreme Court exercises appellate jurisdiction through which it has the power to withdraw cases from the HighCourtregardingcriminalmatters.TheappealagainsttheorderoftheDistrictCourtcanbefiledintheHighCourtofthe State.

ThehierarchyoftheCriminalCourtsinIndiaisgiveninSection6oftheCriminalProcedureCode,1973whichis given as follows:

1. SessionCourt
2. JudicialMagistrateofthefirstclass
3. JudicialMagistrateofthesecondclass
4. ExecutiveMagistrate

SessionCourt

The lowest court of appeal in the hierarchy of Criminal Court is the Court of sessions where the sessions judge conducted the trial. Section 9of CrPC empowers the State Government to establish a Session Court for every sessions division. The High Court appoints the judge of Session Court. Additional Session Judges and Assistant Session Judges can also be appointed by the High Court to exercise jurisdiction in a Session Court.

This Court deals with cases related to theft, murders, dacoity etc. Session Court is empowered to provide a sentence of death and can impose fines for a criminal offence.

The High Court can appoint the Sessions Judge of one division to be an Additional Sessions Judge of another division. When the office of the Sessions Judge left vacant due to some reasons then the High Court has the power to do arrangements for the disposal of any urgent case. If any case is pending before the Session Court then Additional or Assistant Sessions Judge shall have jurisdiction to deal with such a case and in a situation wherethereisnoAdditionalorAssistantSessionJudgethenChiefJudicialMagistrateinthesessionsdivisioncan deal with such application.

SubordinateJudgeClassI

Section11of theCrPCprovidedthat theStateGovernmentcanestablish theCourtof Judicial Magistrateof the first class in the district and any number by consulting with the High Court of the respective State.

ItisgiveninSection15of theCrPCthataJudicialMagistrateissubordinatetotheChiefJudicialMagistrateand it is subject to the control of the Sessions Judge.

Section29oftheCrPCempoweredtheJudicialMagistrateofFirstClassthathemayimposeafinenotmorethan ten thousand rupees or may pass a sentence of imprisonment for not more than three years.

SubordinateJudgeClassII

Section11oftheCrPCempoweredtheStateGovernmentthatitcanestablishtheCourtofJudicialMagistrateofthesecond class in the district and in any number by consulting with the High Court of the respective State.

Section 29(3)of the CrPC empowered the Judicial Magistrate of Second Class that he may impose afine of not more than five thousand rupees or may pass a sentence of imprisonment for not more than one year or both.

Itis incorporated inScheduleI and ScheduleII of the Cr.P.C. that theoffences whichare triablebyeither “Any Magistrate” or “Judicial Magistrate of the Second Class” such offences can be tried by a Judicial Magistrate.

ExecutiveMagistrate

Section 20of CrPC empowered the State Government to appoint Executive Magistrates in every metropolitan areaandineverydistrict.IthastheauthoritytoappointoneoftheExecutiveMagistrateastheDistrictMagistrate and itcan appoint any Executive Magistrate as the Additional District Magistrate and such magistrate has the same power as enjoyed by the District Magistrate under CrPC.

If the office of a District Magistrate left vacant then any officer who is succeeding temporarily to the executive administration of the district shall exercise the same power as enjoyed by the District Magistrate under CrPC. TheStateGovernmentisempoweredtogivechargeofasub-divisiontotheExecutiveMagistrate.TheExecutiveMagistrate who got the charge of a sub-division shall be called as Sub-divisional Magistrate.

JurisdictionofCourtsinIndia

CivilCourts

1. Subjectmatterjurisdiction

Under this Court, the Civil Court has the authority to deal with the cases of a particular type and concerning a particular subject matter. For example- cases related to family matters can only be dealt with by the Family Courts and not by NCLT that specifically deals with company matters only.

TerritorialJurisdiction

When a court exercises its powers within its territory then it is called the territorial jurisdiction. This Court can decide within a geographical limit of the jurisdiction of the court and it can not exercise its powers outside the geographical limit. For example, Madhya Pradesh will have jurisdiction to decide matters arising within Madhya Pradesh only and not outside.

PecuniaryJurisdiction

Under this jurisdiction, the Court has the authority to hear and decide the cases on the basis of the monetary value or the amount of the case or the suit in question.

AppellateJurisdiction

Courtswith higher authority have the power to exercise appellate jurisdiction.Under this jurisdiction, the court withhigher authority canreview thecasethathas alreadybeendecidedby alowercourt.Inourcountry,cases are brought in the form of appeal in the Supreme Court and the High Court, both these courts have the power of appellate jurisdiction. They have the power to overrule the decisions of the lower court.

CriminalCourts

TheproceduretoconductthetrialinthecriminalcourtsisprovidedintheCriminalProcedureCode.

- AccordingtoSection177oftheCrPC,theCourthastheauthorityofthetrialofthecaseonlyiftheoffencehas been committed under the jurisdiction of that court.
- Section178oftheCrpc,dealswiththefollowingmatters:

1. Whentheoffencehasbeencommittedinseveralplacesandtheplaceoftheoffenceisdoubtful.
2. Whentheoffenceispartlyatoneplaceandtherestatanotherplace.
3. Whentheoffenceiscommittedatdifferentplacesandcomprisesofseveralacts.

Ifanyoftheabovesituationsarefulfilled,thensuchoffencemaybetriedinacourthavingjurisdictionoveranyofsuchlocal areas.

- UndertheprovisionsofSection179oftheCrPC,itispostulatedthatanyactwhichbecomesoffencedueto any emanating consequences it is valid for trial in the court of proficient jurisdiction.
- AccordingtotheprovisionsofSection180oftheCrPC,whentheactcommittedisanoffence becauseitisrelatedtoanotheroffencethentheplaceoftrialofthecourtisaccordingtotheoffence whichhasbeencommittedfirsthastobeinquiredintoortriedbyeitherof thecourts underwhose jurisdiction the act has been committed.
- According to the provisions ofSection 181(1)of the CrPC, the trial not only commenced in where theoffencewascommitted,butitcanalsobecommencedwheretheaccusedisfound.Italsodeals with the cases when the offence is not committed in a single place.It deals with the following situations:

1. Thetrialofthecourtiscommencedwheretheaccusedisfoundortheoffenceiscommittedwhile performingtheactofdacoity,dacoitywithmurder,thugetc.thethug,ormurderhascommitted.
2. Inthecaseofabductionorkidnappingofaperson,thetrialiscommencedwherethepersonhas abducted/kidnapped or where the person was conveyed or concealed or detained.
3. Incaseofrobbery,extortionortheft,thetrialofthecourtiscommencedwherethestolenpropertyis possessed, delivered or received or the court where the offence has been committed.
4. In the case of criminal breach of trust or criminal misappropriation, the trial has been committed where any part of the property which is the subject matter of the offence has been received or retained, required to be returned or accounted for, by the accused or where the offence has been committed.

- Section182oftheCrPChasprovidedtheprovisionsfortheoffenceswhicharecommittedbylettersetc. If thevictimhasbeendeceivedbytelecommunicationmessagesorbymeansoflettersorif anyoffencecommittedincludescheatingthenthetrialofthecourthasbeencommencedwherethemessages or letters havebeen sent or received and under the local jurisdiction of the court where thepropertyhasbeenreceivedbytheaccusedpersonorwherethepropertyhasbeendeliveredby the person deceived.
- Section183oftheCrPChasprovidedprovisionsfortheoffenceswhichhavebeencommittedduring voyageorjourney.Duringthejourney,whenapersoncommitsanoffenceagainstatravellerorthe thing inrespectofwhichtheoffence hasbeencommittedisinduecourseofitsvoyageorjourney,

thetrialofthecourthasbeencommencedunderthelocaljurisdictionwherethepersonorthing has been passed.

- Section185oftheCrPCempoweredtheStateGovernmenttodirectanycasesorclassofcasescanbetriedin a Sessions Court for which the trial has been committed in any district.

- Section 186of the CrPC empowered the High Court to resolve the confusion when the cognizanceof a particular offence has been taken by more than one court and confusion arises that which of the Courts shall inquire into or try that offence.

- Section187of theCrPCempowers the Magistrate to issuewarrantor summonsfor offenceswhich do not come under the local jurisdiction of it. In this condition, the Magistrate has the power to order such a person to be produced before him and then send him to the Magistrate of proficient jurisdiction.

- Section 188of the CrPC has provided provisions for the offences which are committed outside the territoryofIndia.Accordingtotheprovisionsof thissection,if anoffenceiscommittedoutsidethe territory of India:

1. ByanIndiancitizen,whetheronthehighseasorelsewhere.
2. Byaperson,notbeingacitizenofIndia,onanyshiporaircraftregisteredinIndia.

This offence is considered as such offence which had been committed at any place within the territory of India and at a place where such person may be found.

- Section189oftheCrPCprovidestheauthoritytotheCentralGovernmentthatitcantakethereceipt of evidence for the offences which are committed outside the territory of India.

JurisdictionofSupremeCourtinIndia

OriginalJurisdiction

Under this jurisdiction, the Court refers to a matter for which that particular court is approached first. Article131of the Indian Constitution gives power to the Supreme Court to resolve the dispute which arises between the States of India or between the State Government and the Union Government.

Article 32of the Indian Constitution empowered the Supreme Court to exercise original jurisdiction in case of infringement of the Fundamental Rights.

AppellateJurisdiction

The power to exercise appellate jurisdiction lies with the Higher Courts. Through this jurisdiction, courts have the power to review, amend and overrule the decisions of the lower courts.Article 132,Article133andArticle134of the Indian Constitution deals with the Appellate Jurisdiction of the Supreme Court in appeals from the high courts in these cases:

1. IftheHighCourtcertifiesthatthesubstantialquestionoflawisraisedinthecaseanditneeds interpretationof the Constitution in Constitutional matters.
2. IftheHighCourtcertifiesthatthesubstantialquestionoflawofgeneralimportanceinvolvedinthecasein civil matters.
3. Ifincriminalmatters,theHighCourthaswithdrawnthecasefromtheSubordinateCourtandon appeal reversed the order of acquittal of an accused and sentenced him to death.
4. IftheHighCourtcertifiesthatthecaseisaworthappealtotheSupremeCourt.

Inanyofthecases,whetheritisofcriminal,civiloranyotherproceeding,ifthecaseinvolvestheinterpretation of the ConstitutionthentheSupremeCourthasthefinalauthoritytoelaboratethemeaningandtheintentofthe Constitution.

AdvisoryJurisdiction

Underthisjurisdiction,thePresidentofIndiacanpleatheadviceoftheSupremeCourttogiveitsopiniononany issueoflaworact.Article143oftheIndianConstitutionempowersthePresidentofIndiatoseekthe opinionof theSupremeCourtonanyissueofpublicimportance.ButtheSupremeCourtcanonlyadviseonthatissue,thatopinionis not binding on the President.

Specialleavepetition

Article136oftheIndianConstitutionempoweredtheSupremeCourttograntspecialleaveagainstthejudgement ortheorderpassedbyanycourtwithintheterritoryofIndia. Article262oftheIndianConstitutionprohibitsthe SupremeCourtfromhearingtheissuesrelatedtointer-stateripariandisputesandpowerofspecialleavepetitiongranted to the Supreme Court has been frequently used to prevent this bar.

Courtofrecord

InIndia,theSupremeCourtisconsideredasa"*CourtofRecord*".ThejudgementsoractspassedbytheSupreme CourtofIndiaareapprehendedaslegalreferencesandlegalprecedents.TheSupremeCourtisacourtofrecord because its judgements are of evidentiary value and cannot be questioned in any court.

JurisdictionofHighCourtinIndia

OriginalJurisdiction

In several cases, people can directly approach to the High Court of India without appeal and this is known as original jurisdiction. The High Court enjoys the power of the original jurisdiction in the following cases:

1. IfthereisadisputebetweentheLegislativeAssemblyandtheMembersoftheParliament.
2. Inmattersrelatedtocontemptofcourt,marriageetc.
3. IncaseoftheinfringementoftheFundamentalRights.
4. Ifthecaseinvolvesthequestionoflawwhichthecourtitselftransferredfromtheothercourt.

WritJurisdiction

Article 226of the Indian Constitution grants powers to the High Court to issue directions,writs or orders in the name of Certiorari, Habeas Corpus, Mandamus, Prohibition or Quo Warranto. The High Court can issue writs in the matter of the Fundamental Rights and other matters also which lie within its territorial jurisdiction.

AppellateJurisdiction

TheHighCourtisconsideredastheprimarycourtofappealbecauseitisempoweredtohearappealsagainstthe judgementgivenbytheSubordinateCourtswithinitsterritorialjurisdiction.Itcanexerciseappellatejurisdictioninthe matters of criminal jurisdiction and civil jurisdiction. The judgements related to Sessions Court and Additional Sessions Court comes under the criminal jurisdiction and the cases involving confirmation of death sentence, imprisonment for seven years awarded by session court before execution. The orders and the judgements ofthe District Courts, Additional District Courts and other Subordinate Courts come under the civil jurisdiction.

SupervisoryJurisdiction

Article227oftheIndianConstitutionempoweredtheHighCourtwiththepowerofsuperintendenceoverallthe courts which come under its territorial jurisdiction except tribunals or military courts which deals with armed forces. The High Court covers both judicial and administrative superintendence. It is not necessary that the appealcamebeforetheHighCourtontheapplicationofapartyonly,itcanbe"***suomoto***"whichmeans"*onitsownmotion"*.

JurisdictionofDistrictCourtandAdditionalDistrictCourt

The District Court or Additional District Court empowered with both original jurisdictions as well as appellate jurisdiction in civil and criminal cases which lies within that district. Civil Courts are governed by the procedure of the Civil Procedure Code and Criminal Courts are governed by the Criminal Procedure Code. In some cases, District Courts have the power of original jurisdiction in both civil and criminal matters, these cases cannot be tried by a lesser court than the District Court.

Civil Courts exercise the power ofSubject Matter Jurisdiction, Territorial Jurisdiction, Pecuniary Jurisdiction and Appellate Jurisdiction. As per the Criminal Procedure Code, a sessions judge of District Court can reward a maximum sentence to the convict is capital punishment.

The District Courtexercisesthe power of appellate jurisdictionover the SubordinateCourts in both thecriminal aswellascivilcases.SeniorCivilJudgeCourt,PrincipalJuniorCivilJudgeCourtandJuniorCivilJudgeCourtare the Subordinate Courts in civilcases.Chief Judicial Magistrate, First Class Judicial Magistrate Court and Second ClassJudicialMagistrateCourtaretheSubordinateCourtsincriminalcases.Theappealagainsttheorderofthe Supreme Court can be filed in the High Court of the concerned state.

JurisdictionofSubordinateCourt

TheCodeofCriminalProcedureprovidedprovisionsforthejurisdictionincriminalmatters.

Section 14of the CrPC deals with the local jurisdiction of Judicial Magistrates. This section empowers the Chief Judicial Magistrate, who is subjected to the control of the High Court that he can define the local limits of the areas from time to time, within which the Magistrates exercise all or any of the powers with which they are invested under this code:

1. ItisprovidedthattheSpecialJudicialMagistrateCourtmayholditssittingatanyplacewithinits local jurisdiction.
2. Iftheexceptionisprovidedbysuchdefinitionthenthepowersofthe Magistrateanditslocaljurisdictionshall extend throughout the district.

3. WherethelocaljurisdictionofaMagistratehasbeenextendedbeyondthedistrictofits jurisdiction or the metropolitan area, as the case may be in which he generally holds court, any reference in thiscode to the Court of Session, Chief Metropolitan Magistrate or the Chief Judicial Magistrate, in relation to such magistrate, throughout the area which comes under his local jurisdiction, be interpreted, unless the circumstances otherwise requires, as a reference to the Court of Session, ChiefJudicialMagistrate,orChiefMetropolitanMagistrate,asthecasemaybeexercisingjurisdiction in relation to that district or metropolitan area.

Section 22of the CrPC deals with the local jurisdiction of Executive Magistrates. This section empowered the DistrictCourt,whichis subjected to the controlof theStateGovernment,thatitcandraw the locallimits of the areasunderwhichtheExecutiveMagistratesmayusealloranyofthepowerswithwhichtheymaybeendowed under this code but there are exceptions when the powers and jurisdiction of such Magistrate shall extend throughout the district.

Section 27of the CrPC deals with the jurisdiction in the case of juveniles. If the accused is under the age of sixteen years then the case is tried by the Court of the Chief Judicial Magistrate or by any court which is tried under the Children Act, 1960.

Section177toSection189oftheCrPCdealswiththeprovisionsrelatedtoinquiriesandtrialsofthejurisdictionofthe Criminal Courts.

Section177oftheCrPCprovidesthatthecourtwhichcomesunderthe localjurisdictionwheretheoffencehas been committed then that offence must be inquired and tried by that court.

Section178oftheCrPCdealswiththeprovisionsrelatedtotheplacewheretrialorenquiryofoffenceshouldbecommenced when there is uncertainty regarding the place of commencement of offence.

Section179oftheCrPCprovidesthatthetrialoftheoffenceiscommencedattheplaceoftheactwhereitis done or the place where the consequence ensues.

Section180oftheCrPCprovidedtheprovisionsforaplaceof trialinasituationwhereanactbecomesoffence due to another offence.

Incaseofcertainoffences,Section181oftheCrPCprovidesprovisionsfortheplaceoftrialforsuchoffences.

Section182oftheCrPCdealswiththeoffenceswhicharecommittedbytelecommunicationmessagesorbyletters etc.

Section183oftheCrPCdealswiththeoffenceswhicharecommittedduringjourneyorvoyage.

Section184oftheCrPCdealswiththeoffenceswhicharetriabletogetherandprovideprovisionsforsuchoffences.

Section185oftheCrPCempoweredtheStateGovernmentto directanycasesorclassofcasescanbetriedin a Sessions Court for which the trial has been committed in any district.

Section186oftheCrPCempoweredtheHighCourttodecidethedistrictwherethetrialorinquiryof offenceshould be commenced in cases where there is confusion regarding the place of trial.

Section187oftheCrPCempowerstheMagistratetoissuewarrantorsummonsfortheoffencewhichiscommittedbeyond the local jurisdiction.

Section188oftheCrPCdescribestheoffenceswhicharecommittedoutsidetheterritoryofIndia.

Section189oftheCrPCprovidestheauthoritytotheCentralGovernmentthatitcantakethereceiptofevidenceforthe offences which are committed outside the territory of India.

TheCodeofCivilProcedure,1908,providedprovisionsforthejurisdictionincaseofcivilmatters.

Section15oftheCPCprovidesthatthesuitfortheoffencefirstlyhavetobeinstitutedintheCourtofthelowest grade competent for the trial.

Section16oftheCPCprovidedthatwheresuitshavetobeinstituted,shouldbebasedonthesubjectmatter which is subject to the pecuniary or other limitations prescribed by the law.

Section17oftheCPCprovidedthatthesuitsfortheimmovablepropertyhavetobefiledwithinthelocallimitsof whose jurisdiction where any part of the property is situated.

Section18oftheCPCprovidedprovisionsfortheplaceofinstitutionofthesuitwherelocallimitsofthejurisdictionofCourts are uncertain.

Section20oftheCPCprovidedprovisionsfortheplaceofinstitutionofothersuits. Itstatesthat suitsforthe offence have to be instituted where the cause of action arises or at the place where the defendants reside.

IntroductiontoCyberspace

Two decades ago, the termcyberspace seemedrightoutof ascience fictionmovie.In the second decade of the twenty-firstcentury,cyberspaceisprobablytheplacewheremostofusspendamajorpartofourlives.Ithasbecomeaninseparableelementofourexistence.Inthisarticle,wewilllooka whatformscyberspaceandthereasonswhylawsareimportanttoensurecybersecurity.

IntroductionofInformationTechnologyAct2000

WhatisCyberspace?

Wehaveallseenthattechnologyisa greatleveler.Usingtechnology,wecreatedmachine-clones– computers,whicharehigh-speeddataprocessingdevices.

They canalso manipulate electrical,magnetic,andopticalimpulsesto perform complexarithmetic,memory,andlogicalfunctions.Thepowerofonecomputeris thepower ofall connectedcomputerstermedas anetwork-of-network ortheinternet.

Cyberspaceisthedynamicandvirtualspacethatsuch networks ofmachine-clones create.Inother words,cyberspaceisthewebofconsumerelectronics,computers,andcommunicationsnetworkwhichinterconnecttheworld.

Source:Pixabay

BrowsemoreTopicsunderCyberLaws

- CyberAppellateTribunal
- DigitalSignature
- RegulationofCertifyingAuthorities

- ClassificationandProvisionofCyberCrimes
- ScopeofCyberLaws
- ElectronicRecordandE-Governance
- InformationTechnologyAct,2000

HistoryofCyberspace

In1984,WiliamGibsonpublishedhisscience fiction book– Necromancer,whichdescribesanonlineworldof computersandelementsofthesocietywhousethesecomputers.Thewordcyberspacefirstappearedinthisbook.

Inthebook,ahackerofdatabasesstoledataforafee.Theauthorportrayedcyberspaceasathree-dimensionalvirtuallandscape.Also,anetworkofcomputerscreates this space.

Accordingtohim,cyberspacelookedlikeaphysicalspacebutwasactuallyacomputergeneratedconstruction.Also,itrepresentedabstractdata.

The bookcaughttheimaginationofmanywritersandin1986,majorEnglishlanguage dictionariesintroducedtheword‘cyberspace’.AccordingtotheNewOxfordDictionaryofEnglish,‘CyberSpace’isthenotionalenvironmentinwhichpeoplecommunicateovercomputernetworks.

Sincecyberspaceisa virtualspace,ithasnoboundaries,mass,orgravity.Itsimplyrepresentstheinterconnected spacebetweencomputers,systems, and other networks.

Itexistsintheformofbitsandbytes–zeroesandones(0’sand1’s).Infact,theentirecyberspaceisadynamicenvironmentof0’sand1’swhichchangeseverysecond.Thesearesimplyelectronicimpulses.Also,itisanimaginarylocationwherethewordsoftwopartiesmeetinconversation.

Cyberspacevs.PhysicalWorld

Firstly,cyberspaceisadigitalmediumandnotaphysicalspace.Itisaninteractiveworldandisnotacopyofthephysicalworld.Herearesomedifferencesbetweencyberspaceandthephysicalworld:

PhysicalWorld	Cyberspace
Static,well-defined,andincremental	Dynamic,undefined,andexponential
Hasfixedcontours	Isasvastasthehumanimaginationandhasnofixedshape

Ina humanbrain,therearecountless neuronswhichcreateaspectreoflife.Similarly,thecyberspacerepresents millions ofcomputers creatingaspectreofdigital life. Therefore, cyberspaceisa naturalextension ofthephysical world intoan infinite world.

CyberSecurityandCyberLaws

Astechnologyevolved,theneedtoregulatehumanbehaviorevolvedtoo.Cyberlawscameintoexistenceinordertoensurethatpeopleusetechnologyand avoid its misuse.

Ifanindividualcommitsanactwhichviolatestherightsofapersoninthecyberspace,thenitistreatedasacyberspaceviolationandpunishableundertheprovisions of the cyber laws.

Sincethecyberspaceiscompletelydifferentfromthe physicalworld, traditionallawsarenotapplicablehere.Inorderto providecybersecuritytousers,thegovernmentintroducedseveralcyberlaws.

Whentheinternetwasdesignedanddeveloped,thedevelopershadnoideathatitwouldhavethepotentialofgrowingtosuchgreatanextent.

Today,manypeopleareusingtheinternet for illegal andimmoral activities whichneedregulation.Inthecyberspacethingslikemoneylaundering,identitytheft, terrorism, etc. havecreated aneed for stringent laws to enhancecybersecurity.

Additionally,manytechnologicallyqualified criminalslike hackersinterferewithinternetaccountsthroughtheDomainNameServer (DNS),IPaddress,phishing,etc.andgainunauthorizedaccesstoauser'scomputersystemandstealdata.

Whilethereisnocleardefinitionofcyberlaw,itisbroadlythelegalsubjectwhichemanatedfromthedevelopmentoftechnology,innovationofcomputers,use of the internet, etc.

CyberLaw

Cyber Law encapsulateslegalissueswhicharerelatedtotheuse ofcommunicative,transactional,anddistributive aspectsofnetworkedinformation technologies and devices.

ItisnotasdistinctasthePropertyLaworothersuchlawssinceitcoversmanyareasthelawandregulation.Itencompassesthelegal,statutory,andconstitutionalprovisionswhichaffectcomputersandnetworks.

Further,itconcernsitselfwithindividuals,andinstitutionswhich:

- Playanimportantpartinprovidingaccesstocyberspace
- Createhardwareorsoftwarewhichallowspeopletoaccesscyberspace
- Usetheirowncomputersandentercyberspace

CyberLawisagenerictermreferringtoallthelegalandregulatoryaspectsoftheinternet.Everythingconcernedwithorrelatedtooremanatingfromanylegalaspects orconcerninganyactivitiesofthecitizensinthecyberspacecomes withintheambitofcyber laws.

Currently,therearetwomainstatuteswhichensurecybersecurity:

1. TheIndianPenalCode.1860
2. TheInformationTechnologyAct,2000

SolvedQuestiononCyberspace

Q1.Whataretheprimarydifferencesbetweencyberspaceandthephysicalworld?

Answer:Thephysicalworldisstatic,well-defined,andincrementalwithfixedcontours.Ontheotherhand,the cyberspaceis dynamic,undefined,andexponential.Italsoisasvastasthehumanimaginationanddoesnothaveafixedshape.

Webhostingcybersecurityconcerns

Securingyourwebsitefromcyberattacksisbecomingincreasinglydifficult

(Imagecredit:Shutterstock)

It'salready2021,andtechnologyisevolvingbytheday.Gonearethedayswhenoperatingawebsite(orevenacomputer)requiredextensivean d specific knowledge of web development.

Today,buildingandlaunchinganewwebpageboilsdowntochoosingawebsitebuilder,adomainname,andareliablewebhostingplan.Now,thislastoneisessentialf oryour success.

Theright providerwillnotonlyensureyou haveawell-suitedenvironmentforyouronline project - theycanhelpyousecureitaswell.Cybersecurityreportsoutlineagrowingnumberofcyberattacksandunveilconcerningstatisticsaboutthepo tentialdangerslooming over our websites.

- Alsocheckoutourlistofthebestendpointprotection

Thecurrentstateofcybersecurity

Thenumberofwebsitesworldwidestill growsexponentially,andsodoestheincentiveforattackerstotryandbreachthem.Thereasonsfor thatarecountless - profit,competitorespionage,securitytests.Someattackersevendoit forthe funofit, justtoprovetheycan.

Accordingto2020statistics, databreaches havecausedover 36billionrecordstobe exposedjustbythe first halfoftheyear.Thenyouhavethe rising numberof malware andvirusthreats,thegrowing pressureoveressentialsectors likebankingandhealthcare,new strategies like ransomware.

Thepandemicdidn'thelpeither.Asmorepeoplewerestuckatworkingathomebehindtheirscreens,hackersweremoreactivethanever. In fact, cybercrime numbers have increased by a whopping 600% for the last year and a half. Defendingyourwebsiteagainsthackersnowinvolvesintricatestrategiesthatneedtoprotectyourpremisesagainstallkindsofdangers.

Hereareafewofthemostpopulartoolsamongthehackingcommunity.

Commoncybersecurityconcerns

Wehavetogetonethingstraightfromthebeginning.Eventhoughtherearehundredsofdifferentwaysahackercanbreachourpremises,ove r 90% of successful attempts are still a result of our own errors.

Moreandmorebusinesses arerecognizingthe growingthreats,butthemajorityofwebmastersarestillwaybehindwhenitcomestosecuring passwords, hosting accounts, and their site itself.

That'sjustgreatnewsforhackers.Relyingonyourweaksecurity,theycanbesiegeyourwebsitewithaplethoraofmethods.

(Imagecredit:Andriano.cz/Shutterstock)

Malware - this is a broad term that encompasses all kinds of malicious practices that aim to cause damage to yourcomputer,website,orserver.Commontypesofmalwareincludeviruses,trojans,worms,spyware,ransomware,adware,andmanym ore.Malicious filescandisruptyoursysteminmanyways.Someare designedtoretrieveprivateinformationfromthebreachedaccount.Othersdeny administrativeaccesstoessentialcomponents,efficientlylockingyououtofyourownsystem.Thereare even thosethat simply want to erase or destroy anything they can infect.

- Checkoutourroundupofthebestmalwareremovalsoftware

(Imagecredit:wk1003mike/Shutterstock)

Phishing-oneofthemostquicklydevelopingtypesofattacks.Hackersutilizephishingwhentheywanttoappearasalegitimateentity,robbing unsuspecting victims of their personal information.
Phishing attacks often occur via emails or social media messages, posing as banking institutions, telecoms, orgovernmentauthorities.Theywillpromptyoutoupdatesomevitalpieceofinformationbyredirectingyoutoaseeminglylegitpage.Inr eality,you will just be giving hackers your current private details.

Phishingattackscanalsotakedifferentshapesandforms,likewhaling,spearphishing,pharming,andmore.

(Imagecredit:FrameStockFootages/Shutterstock)

DOS and DDoS Attacks - DOS stands for denial-of-service and represents a type of attack where the attacker aims to overloadtheserver, draining it from its available system resources. The system gradually slows down until it becomes completelyinoperable.When we talk about distributed denial-of-service (DDoS) attacks, we depict the process of the hacker using multipleinfectedmachinestoblasttraffictowardtheserver.Again,theideaistotakeyourserverdownandpossiblylaunchmoreattacksafter ward.

Botnets,TCPSYNflood,andping-of-deathareamongthecommontypesofDOSandDDOSthreats.

- HereisourlistofbestDDoSprotection

SQL Injections -this is apopularway forhackersto insert maliciouscode and force it to revealprivate user andadmin data.Theinjectionsaffecttheserverquerylanguage(SQL),soyoucangetenoughcontroloverthemachine.Commentandsearchboxe sareoften a great target for SQL injection attacks.
CrossSiteScripting-duringcross-sitescripting(orXSS),attackersmixmaliciouscodewithcontentfromlegitimatewebsites.Thisallowsthe script totravel all the waytothevisitor'sbrowser andinfect it as well.XSSattacksoftenemploymalicious JavaScriptcode butcan also include HTML, CSS, and flash files as well.
PasswordAttacks -attheendofthe day,our weakpasswordsremainthemostoftencauseofourhacker issues. People arestillusingsimpleandeasy-to-guesslogincredentialsbasedontheir memorability, butthisopensahugedoorwayforunauthorizedattackersto get in. Brute-forceanddictionaryattacksaretwowidespreadbreachingmethods,andoncehackersgetyourpassword-it'ssmoothsailingtowardall your data.

- We'vealsofeaturedthebestpasswordmanager

(Imagecredit:Shutterstock)Whatcanyoudoabo

utyourcybersecurity?

Thesituationmightseemgrim,butluckily,thereisalotyoucandotominimizetheaboverisks,maybeevenwipingthemoutcompletely.Consid er any of the following:

- Settingupafirewall
- Optimizingyourwebsitecode
- Utilizingsecuresoftwareandplugins
- ChangingyouradminusernameandloginURL
- Usingtwo-factorauthentication(2FA)
- Keepingyourowncomputersecured
- ActivatingapasswordmanagementtoolAndthen,ofcourse,yo

uhaveyourhostingproviderrightinthemiddleofit.

A reliablehostappliesseveral layers ofsecurityevenbeforethey accommodateyouraccount -overthe datacenters, thenetwork,theservermachines.Ensuring theenvironmentiscompletelysafebeforetheclients landonitwillonly leaveuserswiththeirownsecurityresponsibilities.

Takingthingsastepfurther,companieslike ScalaHostingdevelopin-housesolutionstofurtherprotectcustomersfrommalwareandspam. SShield, forexample,isan AI-poweredsecuritymonitoringtoolthat detectsover99.998%ofwebattacks,completelyfreefor all managed VPSusers. Speakingofvirtualservers,optingforsuchaplanwillremovealltheobstaclesthatcomewiththestandardsharedhostingenvironment.AVPSwillallowyoufullcontrolov eryourhostingaccount,soyoucanconfigureyoursecuritymeasurestoperfection.

Thinkinglongterm

Today'swebsiteownershavemorethanafewcybersecurityconcernstowraptheirheadsaround.Theincentivesforhackersaregettingmorel ucrative,andevennon-commercial projectsarenotoutofdanger.Pickingupasecurehostandfollowingtherecommendedpractices are a great start but make sure to always have a detailed strategy to avoid problems down the road.

- We'vealsohighlightedthebestantivirus

CybersquattingandDomainNames

Rapiddevelopments andenhancementsininformationtechnologyhavebrought anewplatformfor tradeandbusiness.They haveincreasedtheirsignificanceandpresenceinthe“onlinemarkets”withthehelp of theirtrademarkstoattractconsumers. Hence,inthisscenario,trademarks playanimportantroleincyberspaceandtherefore,increasingtheneedfortheirprotection.

Disputes over rights to domain names, which serve as a source – identifying function in cyberspace, similar to a trademark, ariseattheheartofthisintersectionbetweeninternationaltrademarklawandtheInternet1.Ineffforttoreconciletheuniquecomplexities presented by domain name disputes, a host of vehicles have been developed by which aggrieved parties may assert their rights such as the Uniform Domain Name Dispute Resolution Policy (UDRP) promulgated by the Internet Corporation for Assigned Names and Numbers (ICANN), the nonprofit organization that manages the DNS.2

RoleofDomainName

InternetProtocol(IP) addresses,whichconsistof astringofnumbers separatedbyperiods,areusedtoidentifyInternetsites. Adomainnameprovides acorrespondingalphanumeric addresswhichiseasiertorememberandoftenintuitive.Forexample, www.ibm.com is IBM’s website.3

Accordingly,domainnamesrepresentthesamepurposesastrademarks,online,forbusinessandcommercialpurposes.Theyserveto identify the source of goods and services, such as:
· Promotionofbusinessandbuildingupofcustomerbaseonlineandofflinebywasofadvertisingontheweb.
· EstablishmentofthecredibilityofthewebsiteandthebusinessoftheInternet.
· Easyaccesstocustomersandprospectivecustomers.4

Cybersquatting

Registrationofdomainnamesaredoneon'firstcome–firstserve'basis.Thisgivesrisetomanyproblemsasanypersoncanregisterany domain name of their choice regardless of whether that name holds anytrademark or goodwill of acommercial/business enterpriseor represents any kind of organization. This lead tothereserving of many well knowntrade names, brand names, company names, etc. byindividual/corporations other the ones with a genuine interest inthedomain name, with a view to trafificking/doing business on the said domain name to the genuine buyer5.

Cyber-squatters,alsoknownas"cyber-pirates",beatacompanytothepunchbyreservingacompanynameortrademarkasadomain name in thehope of profiting when the company wants to reserve its own name.6 Essentially, cyber squatters fraudulently obtainthesedomain names with theintent tosellit tothelawful owner of the name at ahigher price or premium. Thecyber squatters quicklysell thedomain names to other non-related entities, thereby enabling passing off and diluting of famous trademark or tradenames.7 Passing off is aform of unfair tradepractices in which one partyseeks toprofit fromthe other party's reputation.

Themainproblemlies inthefactthattwoownerscannothavethesamedomainname.Hence,althoughcybersquatters are notcompletelyrestrictingcorporations fromregisteringanydomainnameoftheirchoice,itcanbearguedthatcybersquatters are not preventingtheright ofcorporations todomainnames.However,byregisteringthemostobvious as adomainname(e.g.,the name of the corporation itself), cyber squatters force corporations to find other ways to attract consumers totheir Internet pages8. Instead of simplytyping an obvious domain name for a corporation, customers are forced to use a search engine, whichmaycauseadditional confusionor delay when accessing the desiredsite.9 Moreover, with theprogramming of search engines, often enough websites of the competitor's with similar domain names pop up.

Consumersseekingthepageofaspecifiedtrademarkownerwilllikelyturntoasearchenginebecauseaninitialattemptoftypinginthe domain name (For example, 'www.trademark.com') does not yield the desired result as acyber squatter has already registered that domain. Therefore, the trademark owner is injured in three ways10:

1. Usingasearchenginewillinconveniencetheconsumer,becausehemaypossiblyhavetowadethroughthousandsofothersitesto gettothedesiredsite.Thus,this increases thecustomerssearchcosts andmakes itmorelikelythatthecustomerwillbecome frustrated with the trademark owner, regardless of the quality of her products or services.

2. Thesearchengineroutelikelywillbringupmanyİnternetsitesofthetrademarkowner'scompetitors.

3. Thefrustrationthatcustomersfacewiththis problem mayconvincecustomerstousealternative,non-Internetmeans toget the desired products. This fact, combined with the likely frustration from the search engine process might make customers, originallysearchingtopurchasethetrademarkowner's products,shifttheirpurchasestothetrademarkowner's competitors.11

Consequently,protectingdomainnamesanditsidentityhasbecomeimportant.
The cases sofar, have showed that the conflicting issue in related to the use of the goodwill of a trademark by an infringerin thedomainnametodivertthecustomers orpotentialcustomersoftheownerof thetrademarktoawebsitenotassociatedwith that trademark, oruseof metatagsresultingindilutionof trademark orunauthorizedregistrationofthetrademarkas domainname with the intent to extort money or to prevent the owner from using the trademark.12

Lawrelatingtodomainnamesandcybersquatting

Uniform Domain Name Dispute Resolution Policy(UDRP) is an internet-based system that resolves complaints made by owners of trademark when facing trademark conflict. Being neither a court nor an arbitration authority it controls deletion/ transferofdomainnames.Accordingtothepolicy,acomplainantcanbringactionongrounds includingadomainnamebeing identical/confusinglysimilarto atrademark/servicemark,domain nameowner has no rights/legitimateinterests inthesame or the domain name so registered is being used in bad faith. After the approval of all thesestipulations the registration is proved, or domainregistrationcancelled/transferredtocomplainant.However, nofinancialremedies areapartoftheUDRPmechanism.

UDRP is definedas an "expedited administrative proceeding", and under it the trademark holdercomplaints tothe approved dispute resolution provider. UDRPmay also be referred to as alegally qualifiedspecific contract term. For country-codetop-leveldomainslike.ukand.de,UDRPappliesonlyifthecountryadministratorvoluntarilyadoptsit.Generictop-leveldomainslike.com and.org are under UDRP's scope. It is acheap, fast and easyalternative tocomplexcourt procedures and long hours.
WIPO is the most important dispute-resolution service provider under the UDRP, accredited to ICANN for domain names. It providesskilledpanelists,thoroughadministrativeproceduresandcompletecredence.IttakesabouttwomonthsforaWIPOcasetobe resolved, with a small fee to be made. A case with higher complexity may be heard in person.13

ApersonmaycomplainbeforetheadministrationdisputeresolutionserviceproviderslistedbyICANNunderRule4 (a)that:
(i) Adomainnameis"identicalorconfusinglysimilartoatrademarkorservicemark"inwhichthecomplainanthasrights;and
(ii) Thedomainnameowner/registranthasnorightorlegitimateinterestinrespectofthedomainname;and
(iii) Adomainnamehasbeenregisteredandisbeingusedinbadfaith.

RoleoftheJudiciary

In India, currently, thereis no legislation or provision relating to disputes with regard to domain names or cybersquatting therefore,theTrademarksActplaysaninfluentialroleindecisionsofthecourt.Unlikeothercountriesthathaverecognizedthismenace, India has only relied upon the precedents of the courts.

However,inthecaseof**SatayamInfowayv.SiffynetSolutions**14,theHon'bleSupremeCourtindicatedtotheneedfordomain,as follows:

"Theoriginal roleof a domain name was no doubt toprovide an address for computers on theInternet. But theInternet has developedfromameremeans ofcommunicationtoamodeofcarryingoncommercialactivity.Withtheincreaseofcommercial activityontheInternet,adomainnameisalsousedasabusinessidentifier.Therefore,thedomainnamenotonlyservesasanaddressfor Internet communication but also identifies the specific Internet site. In the commercial field, each domain name ownerprovides information/servicesthat areassociated withsuchdomainname.Adomainnameis easytorememberanduse, andischosenasaninstrument ofcommercial enterprisenot onlybecauseitfacilitatestheabilityofconsumerstonavigate theInternettofindwebsitestheyarelookingfor,but alsoatthesametime,servestoidentifyanddistinguishthebusiness itself, or its good or services, and tospecifyits corresponding online Internet location. Consequently a domain name as an address must, of necessity, bepeculiar and unique and where adomain nameis used inconnection with a business, the value of maintaininganexclusiveidentitybecomescritical.”15

Moreover,incaseofRediffCommunicationvCyberbooth15thecourtdecidedthatthevalueandimportanceofadomainname is equitabletobeinglikethecompany’s asset andtherefore,domainnames mustbetreatedlikecorporateassets andmustalso be protected as such, similar to trademarks.

YahooIncv.AkashArora17wasanothersuchcasewheretheplaintiffsoughtpermanentinjunctiontorestrainthedefendantsfromusing the trademark or domain name yahooindia.com or such deceptively similar to the trademark “Yahoo” for any commercial purposes. Thedefendants argued that as Yahoo was not trademarkedinIndia,thereis noinfringement, as it did notfall under thedefinition of goods underIndianTrade Marks Act,1958. Yet,the plaintiff was granted the injunction, as services rendered on Internet are globally recognized as goods and Yahoo’s trademark ought to be protected.

Astherearenospeciallawsorstatutestopreventcybersquattingin India,theprincipleofpassingoffisprimarilyapplied.

AswasseeninthecaseofTataSons LtdVManuKosuri18,Tata’strademarkwasmisappropriated.Thedefendantregistered many domainnamesincorporatingthetrademarkTata.Thecourtheldas domainnames arevaluablecorporateassets,theyare entitled to trademark equivalent protection.

References:

1. Singh,Bhavna,“CyberquattingandDomainNameDisputes;UndertheTrademarkLaw”,p.6
2. LisaM.Sharrock,“TheFutureofDomainNameDisputeResolution:CraftingPracticalInternationalLegalSolutionsfrom within the Journal, Vol. 51, No. 2 (Nov., 2001), p. 817-849UDRP Framework”, Duke Law
3. Golinveaux,Jennifer,“What’sinaDomainName:Is“Cybersquatting”TrademarkDilution”,33U.S.F.L.Rev.6411998–1999,p. 641
4. Singh,Bhavna,“CyberquattingandDomainNameDisputes;UndertheTrademarkLaw”,p.7.
5. Singh,Bhavna,“CyberquattingandDomainNameDisputes;UndertheTrademarkLaw”,p.8.
6. Golinveaux,Jennifer,“What’sinaDomainName:Is“Cybersquatting”TrademarkDilution”,33U.S.F.L.Rev.6411998–1999,p. 641.
7. ManishVijv.IndraChugh,AIR2002Delhi243
8. Mercer,JohnD.,“Cybersquatting:BlackmailontheInformationSuperhighway”.
9. Ibid
10. Mercer,JohnD.,“Cybersquatting:BlackmailontheInformationSuperhighway”.
11. ibid
12. Singh,Bhavna,“CyberquattingandDomainNameDisputes;UndertheTrademarkLaw”,p.10.
13. http://www.wipo.int/amc/en/center/faq/domains.html#7,accessedonApril18,2014
14. AIR2004SC3540
15. ibid
16. AIR2000Bom27
17. 78(1999)DLT285
18. 90(2001)DLT659;2001PTC432

This article has been Awarded CertificateofExcellenceforOriginalLegalResearchw orkbyourPenal of Judges

Intern tAccess?

CompanyemployeesneedaccesstotheInternettodotheirjobs.However,asremoteandhybridworkpoliciesbecomecommonplace, employees are no longer consistently protected by an organization’s on-prem securitysolutions.

Employees both remote and in the officefacea rangeof threats from the public Internet. Phishing sites attempt to steal sensitiveinformationanddelivermalware.SensitiveinformationmaybeinsecurelysharedonunapprovedSaaSappsorother sites. Automated bots perform credential stuffing and other attacks.

SecureInternetAccessprotects employees against web-basedthreats andminimizes theriskof databreaches and other threats.Thisisaccomplishedbyinspectingandfilteringnetworktrafficbasedoncorporatesecuritypolicyandthreatdetectionrules.

HowDoesSecureInternetAccessOperate?

SecureInternetAccessisdesignedtoinspectandprotectinboundandoutboundtrafficbetweenauser'smachineandthepublic Internet. This can be accomplished in a couple of ways:

- **In-BrowserProtection:**Agentsdeployedinauser'sbrowsercaninspectInternettrafficontheendpointitself.Thisprovides secure and private web browsing without incurring latency or redirecting traffic to an inspection point.

- **Cloud-BasedProtection:**Asecurewebgateway(SWG)deployedasacloudservicecanprovideprotectiontoan organization'sentireworkforce.Thissolutionworksforalldevices,providingprotectionforthosethatmightbeunable to support in-browser agents.

TheMainProtectionsforSecureInternetAccess

Securebrowsingsolutionsshouldprovideprotectionagainstthemainweb-basedthreatsthatorganizationsface.Theyshould includethe following five core capabilities.

#1.MalwareProtection

Userscanbeinfectedwithmalwareviavariousweb-basedthreats.Malwarecanbedownloadedfromphishingpagesor deliveredviatheexploitationofbrowservulnerabilities.Onceinstalled,themalwarecommunicateswithandreceivesinstructionsfrom attacker-controlled servers via command and controlcommunications (C2C).

Asecurebrowsingsolutionshouldoffercomprehensiveprotectionagainstmalware.Alldownloads shouldbeinspectedfor maliciouscontentinasandboxedenvironmentandbesanitizedusingcontentdisarmandreconstruction(CDR).Solutions shouldalsoidentifyandautomaticallyremediatemalwareinfectionsandvirtuallypatchvulnerabilitiesinusers'browsers.

#2.PhishingProtection

Phishingattacksaresomeofthemostcommonandeffectivethreatstocorporatecybersecurity.Asuccessfulphishingattack oftenleadsuserstoawebpagethatstealssensitiveinformationordeliversmalware.

AsecureInternetaccesssolutionshouldleverageartificialintelligence(AI)andheuristicanalysistoidentifyphishingpages. This includes inspection of all form and password boxes and lookingfor a widerangeof potential phishingindicators.

#3.DataLossPrevention

Databreacheshavebecomearegularoccurrence,andthecostofadatabreachtoanorganizationisgrowing.Often,theseleaksare enabled by negligent or malicious employee behavior.

Securebrowsingsolutionsshouldbeabletomanageexposurerisksforsensitivecorporateinformation.Thisincludesblockingsharingor storage of sensitive information on unsanctioned social media, SaaS applications, and file-sharing services.

#4.CredentialTheftPrevention

Credentialstuffingattacksareamajorcyberthreatthatexploitswidespreadpasswordreuse.Credentialsbreachedfromone siteareusedtogainaccesstoanemployee’sotheronlineaccounts.

Asecurebrowsingsolutionshouldprotectagainstthethreat of employees reusingtheircorporatecredentialsforonline applications.Solutionsshouldblocktheentryofcompanypasswordsintowebsitesandalertadministratorsofattemptstodo so.

#5.AccessControl

Thegrowthofremoteworkhasblurredthelinesbetweenpersonalandbusinessdeviceusage.Adultorgamblingwebsitesmayinclude malicious content that puts corporate data and systems at risk.

SecurebrowsingsolutionsshouldincorporateURLfilteringfunctionality.Thisenablesanorganizationtoblockvisitsto inappropriateordangeroussitesandtoprotectagainstdatabreachesbydisallowingtheuseoffile-sharingsitessuchasTorrent.

Miercom
Check Point is #1 in Miercom NGFW Security Benchmark 2023
99.7% Block Rate vs. 72.2% for nearest competitor
GET REPORT

HowtoChoosetheOptimalInternetAccessSecuritySolution

TheoptimalInternetaccesssecuritysolutionprovidesbothrobustprotectionandapositiveuserexperience.Fivecriticalfeaturesofa secure browsing solution include:

- **ZeroDayProtection:**Cybercriminalsarecontinuouslydevelopingnovelmalwarevariantsanddeploying new phishingpages.AsecureInternetaccesssolutionshouldleverageAItoidentifyandblockunknownmalwareand phishing pages.

- **SSLTrafficInspection:**MostInternettrafficisencrypted,andvisibilityintoencryptedtrafficisessentialtoidentifyingweb-basedattacks.AsecurebrowsingsolutionshouldbecapableofinspectingallSSL-encryptedtrafficwithoutadding significantlatency.

- **SeamlessUserExperience:**ManytraditionalsecureInternetaccesssolutions,suchasremotebrowserisolation(RBI),addsignificantlatencyandcanpreventusersfromaccessingcontent.SecureInternetaccess solutions shouldofferlow-latencySSLinspectionanduseCDR tosanitizeinfectedcontent.

- **ScalabilityandSimpleDeployment:**Remoteworkaddsloadonsecurebrowsingsolutionsandmakesthem more difficultforremoteadministratorstomanage.Asolutionshouldbeadaptable,scalable,andeasytodeploytomeetthe evolvingneedsofthebusiness.

- **Privacy:**Somesecurebrowsingsolutionsexposeusers'browserhistoryandtraffictoadministrators.Asecure browsingsolutionshouldprovideprotectionwhileremainingcompliantwiththeGDPRandotherincreasinglystringentdata privacylaws.

SecureInternetAccesswithHarmony

SecureInternetaccessisessentialtoprotectingremoteworkersandenablingthemtodotheirjobs.Tolearnmoreaboutwhattolookfor in a secure browsing solution, check out this buyer's guide.

CheckPointHarmonyofferssecureInternetaccesswithbothoptionsforbothin-browseragents(HarmonyBrowse)andcloud-basedSecureWebGatewayprotections(HarmonyConnect).LearnmoreaboutHarmonyConnectanditscapabilities bysigningupforafreedemo.

UNIT-2

InformationTechnologyAct,2000:

TheInformationTechnologyAct,2000alsoKnownasan**ITAct**isanactproposedbytheIndianParliamentreportedon17thOctober2000.ThisInformationTechnologyActisbasedontheUnitedNationsModellawonElectronicCommerce1996(UNCITRALModel)whichwassuggestedbytheGeneralAssemblyofUnitedNationsbyaresolutiondatedon30thJanuary,1997.Itisthemostimportantlaw in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate orreducecybercrimes.TheITAct has 13chapters and90sections.The lastfour sections that starts from'section91 – section94', dealswiththe revisions to the Indian Penal Code 1860.

TheITAct,2000hastwoschedules:

- **First Schedule** – DealswithdocumentstowhichtheActshallnotapply.
- **Second Schedule** – Dealswithelectronicsignatureorelectronicauthenticationmethod.

The offences and the punishments in IT Act 2000 :
TheoffencesandthepunishmentsthatfallsundertheITAct,2000areasfollows:-

1. Tamperingwiththecomputersourcedocuments.
2. DirectionsofControllertoasubscribertoextendfacilitiestodecryptinformation.
3. Publishingofinformationwhichisobsceneinelectronicform.
4. Penaltyforbreachofconfidentialityandprivacy.
5. Hackingformaliciouspurposes.
6. PenaltyforpublishingDigitalSignatureCertificatefalseincertainparticulars.
7. Penaltyformisrepresentation.
8. Confiscation.
9. Powertoinvestigateoffences.
10. ProtectedSystem.
11. Penaltiesforconfiscationnottointerferewithotherpunishments.
12. ActtoapplyforoffenceorcontraventioncommittedoutsideIndia.
13. Publicationforfraudpurposes.
14. PowerofControllertogivedirections.SectionsandPunishmentsunderInformationTechnologyAct,2000areasfollows:

SECTION	PUNISHMENT
Section43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/networkordeletingdatawithmaliciousintentionswithoutauthorizationfromownerofthecomputerisliableforthepaymentto bemade to owner as compensation for damages.
Section43A	ThissectionofITAct,2000statesthatanycorporatebodydealingwithsensitiveinformationthatfailstoimplementreasonablesecuritypracticescausinglossofotherpersonwillalsoliableasconvictforcompensationtotheaffectedparty.
Section66	HackingofaComputerSystemwithmaliciousintentionslikefraudwillbepunishedwith3yearsimprisonmentorthe fine ofRs.5,00,000 or both.
Section66B,C,D	Fraudordishonestyusingortransmittinginformationoridentitytheftispunishablewith3yearsimprisonmentorRs.1,00,000 fine or both.
Section66E	ThisSectionisforViolationofprivacybytransmittingimageofprivateareaispunishablewith3yearsimprisonmentor2,00,000 fine or both.
Section66F	ThisSectiononCyberTerrorismaffectingunity,integrity,security,sovereigntyofIndiathroughdigitalmediumis liablefor life imprisonment.
Section67	Thissectionstatespublishingobsceneinformationorpornographyortransmissionofobscenecontentinpublicisliablefor imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

AmendmentsandLimitationsofITAct:

Topicscovered:

1. Governmentpoliciesandinterventionsfordevelopmentinvarioussectorsandissuesarisingoutoftheirdesign and implementation.
2. Challengestointernalsecuritythroughcommunicationnetworks,roleofmediaandsocialnetworking sitesininternalsecuritychallenges,basicsofcybersecurity;money-launderinganditsprevention.

AmendmentstotheInformationTechnology(IT)Act

Whattostudy?

- ***ForPrelims:KeyfeaturesoftheITAct,amendmentsproposed.***

- ***ForMains:Significanceandtheneedforamendments,concernsassociated.***

Context:Initsbidtocrackdownonspreadoffakenewsandrumourscirculatedononlineplatformslike WhatsApp,Facebookandother onlineplatforms,the***centralgovernmenthasproposedstringentchangesunderthedraftof Section79oftheInformation Technology (IT) that govern online content***.

Implications:

Theproposedamendmentsinthedraft of ***theInformationTechnology[IntermediariesGuidelines(Amendment)Rules] 2018,Rule3(9)***isboundtoforcesocialmediaplatforms likeWhatsapp,Facebook andTwittertoremainvigilandkeepusers on their toes before posting or sharing anything that is deemed as “unlawful information or content”.

Thechangesproposedbythecentralgovernmentis***aimedatcurbingfakenewsorrumoursbeingspreadonsocialmediaand check mob violence ahead***.

Whatthenewrulespropose?

Thechanges willrequire***onlineplatformstobreakend-to-endencryptioninorder toascertaintheoriginof messages***. Thesocialmediaplatformsto“deploytechnologybasedautomatedtools orappropriatemechanisms,withappropriatecontrols, for proactively identifying or removing or disabling access to unlawful information or content”.

Aspertheamendment,***thesocialmediaplatformswillneedtocomplywiththecentralgovernment“within72hours”ofaquery***.

Thereshouldbe***a‘NodalpersonofContact***for24X7coordinationwithlawenforcementagenciesandofficerstoensurecompliance. The social media platforms will be keeping a vigil on “unlawful activity” for a period of “180 days”.

Whatnecessitatedthis?

Withconcerns over“risingincidents of violenceandlynchinginthecountryduetomisuseofsocialmediaplatforms”,there is nowneedforonlineplatformstoshoulderthe“responsibility, accountabilityandlargercommitmenttoensurethatitsplatform is not misused on a large scale to spread incorrect facts projected as news and designed to instigate people to commit crime”.

Criticisms:

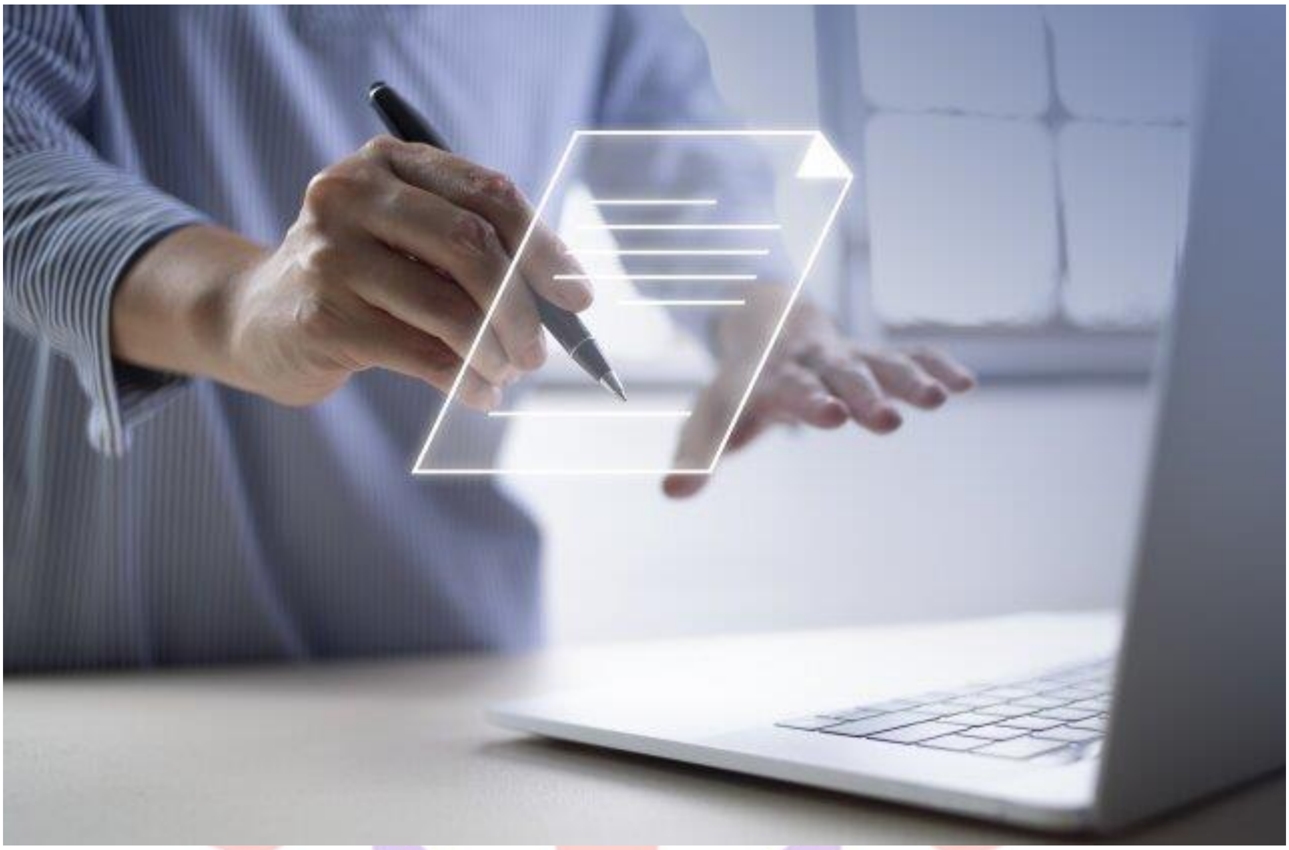
The proposed changes have once again given rise to a debate on whether the government is intruding intothe privacy of individuals, evoking sharp responsefrom opposition parties. Similarapprehensions were raised with the Section 66A of the IT Actthatenabledauthoritiestoarrestusersforpostingcontentwhichwastermedasoffensive.However,theSupremeCourtonMarch24, 2015, struck down the law.

Background:

Indiahasthesecondhighestnumberofinternetusersintheworldafter China,anestimated462.12million.Amongthem, 258.27millionwerelikelytobesocialnetworkusersinthecountryin2019.

DigitalSignature:

Adigitalsignatureisatypeofelectronicsignaturethat’ssecureandcanbeauthenticated.Digitalsignaturesareimportantbecausethey'relegallyenforceablejustlikeahandwrittensignature.They'reusedtosignimportantdocumentslikemortgagedocuments.Asaresult,they'renotthesamethingassimplytypingyourname onanelectronicdocument.Inthisguide,weexplainmoreaboutwhatdigitalsignatures are, how they work, and the benefits they offer.



DefinitionofaDigitalSignature

A digital signature is a type of electronic signature. It's used as a cybersecuritymeasure to encrypt a document to ensureitsauthenticity.AccordingtotheCybersecurityandInfrastructureSecurityAgency(CISA),“Digitalsignaturescreateavirtualfingerprintthatisuniquetoapersonorentityandareusedtoidentifyusersandprotectinformationindigitalmessagesordocuments. Inemails,the emailcontent itself becomes part of the digital signature.”

Encryption is a key part of a digital signature. It prevents documents from being altered by hackersor other bad actorsandauthenticates the signer.

“Adigitalsignatureisanelectronicsignatureand[publickeyinfrastructure]-basedcertificate(digitalID)combinedintoone,”explainsLilaKee,chiefproductofficerandgeneralmanager,AmericasforGlobalSign,aproviderof digitalsignatures. “Theyprovideintegrityand,withtheuseoftrusted,digitalcertificates,authenticitytodigitalmessagessuchasemail,documentsandcodedistributedviatheInternet.”

HowDoesaDigitalSignatureWork?

Beforeyoucanuseadigitalsignature,youmustfirsthaveadigitalsignaturecertificate.“Thiscertificateisapersonalkeythatencryptsthedocumentsandguaranteestheirsafety,”saysSergeyBarysiuk,chieftechnologyofficer(CTO)ofPandaDoc,aproviderofdigitalsignatures.

Adigitalsignaturecertificatealsohaspertinentinformationabouteachuser,includingtheirname,emailaddress,andlocation.Thecertificate can be stored on a hard drive so that only the user can access it.

Whenausersignsanewdocumentwiththeirdigitalsignaturecertificate,thedocumentis"hashed,"ortranslatedintoacode,Barysiukexplains .Thedocument isthenencryptedwiththe user'sprivatekey.

Byhashingadocumentandencryptingitwithaprivatekey,thedigitalsignatureprocesseffectivelycreatesachainofcustody.Thismeansthatchangescan’tbemadetothedocumentwithoutallsignersknowingaboutthem,andsignerscan'tdenyhavingsignedthedocument.

"Theseextrastepsare whatmakesa digitalsignaturemoresecurethananelectronicsignature,"Barysiuksays. "Insteadofjustusingasymbol, it contains your personal key, which verifies the validity of the document.” Effectively, the digital signature serves asanelectronic fingerprint of the signer.

Whiletheprocesssoundscomplicated,itdoesn’tneedtobe.Forexample,MicrosoftincludesadigitalsignaturecapabilityinitsOfficeproductsWord and Excel.

ClassesandTypesofDigitalSignaturesTherearethreebasictypesofdigitalsignatureswithdifferentlevelsofsecurity

:StandardorSimpleElectronicSignatures

Thisisthemostbasicformofane-signature,wherethesignerdrawsortypestheirname,butwithoutanyvalidation.Thiscanincludesimplypastingacopyofawrittensignatureona documentortypingthe user'sname.Typinginafancy,script-like fontdoesn'tmakethis kind of e-signature any more official.

AdvancedElectronicSignatures(AES)

Thistypeofdigitalsignatureuniquelyidentifiesthesignerusingelectronicsignatureverificationdatatowhichonlythesignerhasaccess.

QualifiedElectronicSignatures(QES)

AstricterformofAES,BarysiuksaysQESisaccompaniedwithaqualifieddigitalcertificateandhasthesamelegalvalueasahandwrittensignature.Thistypeofcertificateisissuedbyaqualifiedtrustserviceproviderthatmustbeonthe EuropeanUnionTrustList(EUTL).

Althoughtherequirementsfordigitalsignaturesarebasedon EuropeanUnion(EU)standards,they'reusedintheU.S.andelsewhere.TheU.S.israpidlydevelopingitsowndigitalsignaturesolutions,saysJohnGruetzner,chiefoperatingofficerofSyngrafii.

HowToCreateaDigitalSignature

Creating a digital signature requires generating a public and private key pair using a cryptographic algorithm, says VaclavVincalek,founder and CTO at the virtual CTO firm 555vCTO. The private key is used to sign a document or message, which is thenencrypted.The signed data can then be sent, and the recipient verifies its authenticity using the public key.

As previously noted, you also need a digital signature certificate. Depending on the level of security involved, you can getthiscertificate from a certificate authority.

Ifyoudon'twanttopayorwaitfora digitalsignaturecertificate,youcancreateyourownusingaprocess inMicrosoftWindowsthatwillprovide a certificate. However, other users won't be able to verify it like they would usingone createdby a qualified provider.

BenefitsofDigitalSignaturesDigitalsignaturesareawaytopromotetrustbetweentwopartieswhomustcommunicateelectronicall

y.They

provide a way for the parties to be certain that their communications haven't been altered and that the information they'resharinghas been kept secure.

Relatedbenefitsofdigitalsignaturesinclude:

ImprovedWorkflowsDigitalsignaturesavoidtheneedtocheckandrecheckdocumentsforaccuracyafterthey'vebee

ntransmitted.Security

Adigitalsignatureguardsagainstinauthenticdocumentsbeingpresentedasrealbecauseit'stiedtoaspecificsigner.Itcanalsoguardagainstunauthorizedchangestodocumentsandagainstlossordestruction.Adigitalcertificateobtainedfromalegitimatecertificateauthorityhelpsensure this security.

AuditTrail

Anaudittrailaccompanieseachdocument,makingitpossibletotraceadocumentbacktoitsorigintoverifyit.Eliminationo

fFraud

Thedigitalsignaturepreventsforgeryandothertypesoffraud,including insiderfraud, byusingpublickey infrastructuretoensurethe legitimacy of a document.

UniversalLegality

DigitalsignaturesusestandardsbasedinboththeEUandtheU.S.,anddevelopersensurethattheirdigitalsignaturecodingmeetsinternational standards. This means that digital signatures can be made anywhere and accepted everywhere.

TimeManagement

Oncedigitalsignaturefunctionalityisinplace,thesigningandapprovalprocessisfastandeasy.Thiseliminatesthedelaysandpotential risk of passing paper documents through the approval process.

SocialResponsibility

In addition to reducing or eliminating the paper waste of the document signing process, the use of digital signatures helpscreateconfidence in the security of documents in an organization. This reduces the chance of embarrassing leaksof personallyidentifiableinformation because of lax security or encryption failures.

CostSavings

Theuseofdigitalsignaturescansaveasignificantamountofmoneythatwouldotherwisebespentonroutingandmanagingpaper.Documentmanagementbecomesfasterandstoringdocumentssecurelybecomeseasier.Therearealsocostsavingsinprinting,paper,and secure management of paper documents.

UsesforDigitalSignatures

Digitalsignaturesarealreadywidelyused,especiallyinthehealthcareandfinancialservicesindustries.Otherindustries arestartingto usethem more often as well. Here are some specific examples:

Government

Whenyousignyourtaxreturnonline,you'reusingadigitalsignature.Digitalsignaturesarealsonowappearingongovernmentprocurementdocuments,bills,andevenIDcards.Theprimaryreasonsaresecurity(bogustaxreturnsareahugeproblem)andcost.

HealthCare

Signatures are requiredwidelyinthe healthcare sector foreverythingfrominsurance billingto providingpermissionfortreatment.Security has been a challenge in health care, and digital signatures are a major step in helping with that. Using digitalsignatureseliminates the delays and security issues of paper documents.

Manufacturing

Anumber of stepsin manufacturingrequire signatures, including ordering materials, approvingdesignsand changestodesigns,productionschedules,andstaffingcommunications.Digitalsignaturesmaketheseprocessesmoreefficient.

FinancialServices

Digitalsignaturesarecommoninfinancialservices,especiallyforactivitiesthatcanbeperformedremotely.Thisincludesloansforcars, credit card applications, and other contracts. The banking industry is moving aggressively to digital signatures.

Cryptocurrencies

Digitalsignaturesareusedforblockchainauthenticationwithcryptocurrencies.They'realsousedforverificationof cryptocurrencytransactiondata,wheredigitalsignaturescanalsohelpshowownership.Why

UsePKIorPGPWithDigitalSignatures?

PKI stands for public key infrastructure. "It refers to the system of digital certificates, certificate authorities, and otherregistrationauthoritiesthatareusedtoverify andauthenticatetheidentityofapartyinonlinetransactions,"Vincaleksays.

PGP stands for pretty good privacy. It's a data encryption and decryption program that uses public-key cryptography toprotectinformationfrombeingreadbyunauthorizedparties,accordingtoVincalek.HesaysPKIisgenerallyusedbycorporations,whilePGPisused by individuals.

"UsingdigitalsignaturesinconjunctionwithPKIorPGPstrengthensthemandreducesthepossiblesecurityissuesconnectedtotransmittingpublickeysbyvalidatingthatthekeybelongstothesender,andverifyingtheidentityofthesender,"saysCISA.

Accordingto CISA, the security of adigital signature is almost entirely dependent onhow wellthe privatekey is protected."WithoutPGPorPKI,provingsomeone'sidentityorrevokingacompromisedkey isimpossible;[notusingthem]couldallowmaliciousactorsto impersonate someone without any method of confirmation," the agency says.

DigitalSignaturesvs.ElectronicSignatures

Adigitalsignatureisanelectronicsignaturethatmeetsspecificrequirements,especiallyintermsofsecurity.“Digitalsignaturesworkbyprovingthatadigitalmessageordocumentwasnotmodified–intentionallyorunintentionally–fromthetimeitwassigned,"CISAsays.

Adigitalsignaturedoesthisbyusingthesender’sprivatekeytodevelopthehashthatencryptsthekey.Therecipientusesthesender’spublickeytodecrypttheoriginalmessage,andthencomparesthehashfromeachonetodetermineiftherehavebeenchangestothemessage. If thehashes match, then the message hasn’t been changed.

Electronicsignaturesdon’thavethesesecurityfeatures,meaningthere’snowaytoknowiftheelectronicdocumentwaschanged.Anelectronic signatureis simplya signature that shows uponanelectronic document.A digitalsignature isa secure means of signingadocumentthatallowsyoutoconfirmitsauthenticity,aswell asitsprovenance.To dothis,adigital signaturemustmeettherequirementsoftheElectronic Signatures in Global and National Commerce Act.

TheEUimplemented its firstElectronicSignaturesDirectivein1999, butthatlaw hasbeenrepealedandreplacedwithanupdatedregulation, eIDAS(Regulation on electronic identification and trust services).

Electronicsignatureservicesfrommostvendorscomplywithboth U.S.andtheEUrequirements.

CRYPTOGRAPHYALGORITHMSINCYBERSECURITY:TYPES,EXAMPLES:

Cryptography is one of the oldest and most widely used tools for safeguarding IT assets. Nearly every business relies on cryptographytosecuresensitivedataandITinfrastructure.So, whatiscryptographyincybersecurity,andhowcanithelpyouoptimizeyoursecurityposture?Putsimply, it’s a way to make information unreadable by attackers, even if it is compromised.

WhatisCryptography?

Cryptographyincomputernetwork securityistheprocessofprotectingsensitiveinformationfromunauthorizedaccesswhenitisatrestorintransit byrenderingitunreadablewithoutakey.Leveraging encryption, cryptography helpsuserssecuredatatransmissionovernetworks,ensuringthatonly individuals with designated keys can access encrypted data.

Toanswerthequestion,*whatis* **cryptographyincybersecurity**?,thisblogwill:

- Breakdownthetwotypesofcryptography
- Explaindifferentmethodsofcryptography
- Provideseveralcryptographyexamples
- Walkthroughthebenefitsofcryptographyprotection

Inmostcases,cryptographyneedswillvarydependingonanorganization’sstructure,securitycontrols,andbroadergovernancerequirements.Partnering witha managed security services provider (MSSP) isthe best wayto optimize cryptography protection to your specific needs.

TypesofCryptography

Thereisnoshortageof methodsofcryptographyavailableonthemarket,soyou mightbewonderingwhichcryptographytypes willworkbest for your organization's security needs.

Ingeneral,therearetwotypesofcryptographywidelyusedforcybersecurityapplications:

SymmetricCryptography

Also called "secret key cryptography," symmetric cryptography functions via cryptographic key sharing between users. In this method,thesamekeyisusedtoencrypt anddecryptdataandistypicallysharedbetweenusers. In theory, onlyan individualwith auniquecryptographickeyshould beableto decrypt the encrypted data. Symmetric cryptography is oftenused to safeguard the local storage of sensitive data ondrivesor servers.

AsymmetricCryptography

On another level, *asymmetric cryptography* is typically used to safeguard the transmission of sensitive data across publicnetworks.Asymmetric cryptography is also called "public key cryptography" because its users must have two keys. One of the keys isconsidered a"publickey"thatcanbeprovidedtoanyoneeitherusercommunicateswith.However,thesecondkeydecryptstheencrypteddataandismeantto be kept private.

EncryptionAndDecryptionInCryptography

Sohowexactlydoescryptographywork?Inpractice,aswiththeprimarytypes,therearetwoprimaryapproachesormethodsofcryptography,whichwork hand in hand to secure data:

Encryption

Dataencryptionreferstotheprocessofusinganalgorithmtoconvertbinarydatafromoneformtoanother,accessibleonlybyaspecifickey.Forencryptiontowork,analgorithmconvertsplaintextintoa difficult-to-decipherform(alsocalledciphertext),whichcanonlybeconvertedbacktoplaintextwithacryptographickey.Developingcomplexencryptionalgorithmswillhelpincreasethesecurityofdata transmissionandminimize the risks of data being compromised.

Decryption

Decryptionessentiallyreversesencryption.Usingacryptographickeythat matchestheencryptionalgorithm,ausercandecryptsensitivedatawhether at rest or in transit. Dependingonthecomplexityandrobustnessofthealgorithmsyouuse,bothencryptionanddecryptionincryptographywillhelpoptimizeyour security posture and safeguard sensitive data.

ExamplesofCryptography

With wide-reaching applications,**cryptography** can help secure a wide range of sensitive digital environments, regardless oforganizationsize, businessneeds, orindustry. Yourchoiceofcryptographic solutionswilldepend onthetypeofsecuritycontrols you needtoimplement.Below are some of the **common uses of cryptography:**

EncryptingBYODDevices

Bring Your Own Device(BYOD) policies enable employees to use their own personal phones and computers at work or for work—onpremises and, potentially, for completing work tasks. But BYOD devices are at high risk for security threats if they're used onunsecured,publicnetworks. Theriskofdatabreachesisevenhigherifemployeestransmitsensitivedataonthesedevices. Youshouldconsiderimplementing**BYODdeviceencryption**ifyouremployeescanworkremotelyusingtheirpersonaldevicesorbringthem into work environments altogether.

SecuringSensitiveEmails

Anyemailscontainingsensitivedatashouldbesecuredusingindustry-standardencryptionalgorithmsthatminimizethechancesthatcybercriminalswillaccesstheemails—orbeabletoreadandusedatawithiniftheyareaccessed.End-to-endencryptiontoolscanhelpsecuresensitive emails, especially if private and public keys used to encrypt the emails are kept safe.

EncryptingDatabases

Encryptionalsoextendstodatabasescontainingsensitiveinformationsuchas:

- *Customerdata(e.g.,homeaddresses,bankaccountnumbers)*
- *Employeedata(e.g.,socialsecuritynumbers)*
- *Intellectualproperty(IP)data(e.g.,patentinformation)*

Databaseencryptioniscriticaltomitigatingthreatriskstodataatrestacrosson-premiseandclouddatabases.

ProtectingSensitiveCompanyData

Encryptionisalsoanessentialtoolforsafeguardingyourcompany'ssensitivedatasuchas:

- Employees'personallyidentifiableinformation(PII)
- Financialdatarelatingtothecompanyanditspartners
- CustomerorsupplierdataOneofthemostcommondatabaseencryptiontoolsistransparentdataencryption(TDE),whichencryptsmostSQL-baseddatabases.

HTTPStosecurewebsite

SecurewebsitesaretypicallyencryptedbytheHTTPSprotocol,whichhelpssafeguardtheconfidentiality,integrity,andauthenticityoftransactions on the Internet.

HTTPSencryptionalsohelpsmitigateattackslikeDNSspoofing,wherecybercriminalsattempttodirectuserstounsecuredwebsitestostealtheirsensitiveinformation.HTTPSencryptionisalsowidelyimplementedincustomer-facingindustrieslikeretail,wherecustomerscanimmediately identify an unsecured website based on the "https" in a website's URL.

BenefitsofCryptographyProtection

Cryptographyprotectionkeepsyourdataconfidentialandmaintainitsintegrity.Belowaresomebenefitsofemailencryption,whichcanalso apply to other forms of cryptography:

Confidentiality

Encryptionhelpskeep sensitivedataconfidentialand minimizeanyrisksofthedatabeingexposedtocybercriminals.It isfareasiertoinvestina robustencryption methodthanrisk compromising sensitive data belonging to valuable customers, vendors, or business partners.

Authentication

Whenintegratedintoemailapplications,encryptioncanhelpidentifypotentialphishingattemptsandverifytheauthenticityofemailsenders,links,andattachments.Encryptionwillalsomakeiteasierforyouremployeestoidentifyphishingthreatsandpreventanyfull-blownattacks.

DataIntegrity

Encryptionalsohelpspreservetheintegrityofyoursensitivedata.Specifically,dataissusceptibletosecurityriskswhenit'sstoredlocallyorinthe cloudand during its transmission from one party to another. Using industry-standard encryption algorithms will help keep your datasecure at allstages of storage or transmission.

Non-Repudiation

Cryptography protection can also providenon-repudiationassurance, ensuring both parties receive confirmation of data transmission.Whentransmitting highly sensitive data to business partners, customers, or vendors encrypting your emails will also help avoid any legalissues,should one party claim a message was not sent, received, or processed.

HowRSISecurityCanHelpYouImplementCryptography

Backtothestartingquestion:whatiscryptographyincybersecurity?

It'sasetoftoolstohelpyourorganizationkeepdataandothersensitiveITassetssafe.PartneringwithRSISecuritywillhelpoptimizeyourcryptography,in-houseoroutsourced.Ourcryptographyservicesinclude:

- Localandremotediskencryption
- Implementingencryptionincompliancewithindustrystandards
- Managementofendpointcryptography

- Monitoringtheintegrityoflocalandcloudfilestorage
- Patchmanagementofcryptographytools
- Penetrationtestingofencryptionmethods

AsanexperiencedMSSP,ourteamofexpertsunderstandsjusthowcumbersomeitistomanagetheencryptionofendpointsacrossanorganization.Asthreatskeepevolvingintoday'sITlandscape,wehelpoptimizecryptographyandensurethatencryptiontoolsworkrobustlywithinyour cybersecurity framework.

PublicKeyEncryption

- Read
- Discuss
- Courses

When thetwopartiescommunicatetoeachothertotransfertheintelligibleorsensiblemessage,referredtoasplaintext,isconvertedintoapparently random nonsense for security purpose referred to as **ciphertext**.

Encryption:

The process of changing the plaintext into the ciphertext is referred to as**encryption.**Theencryptionprocessconsistsofanalgorithmandakey.Thekeyisavalueindependentoftheplaintext.

Thesecurityofconventionalencryptiondependsonthemajortwofactors:

1. TheEncryptionalgorithm
2. Secrecyofthekey

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending onthespecifickeybeingusedatthetime.Changingthekeychangestheoutputofthealgorithm.Once the ciphertext is produced, it may betransmitted. Upon reception, the ciphertext can be transformed back to the originalplaintext by using a decryption algorithmandthe same key that was used for encryption.

Decryption:

Theprocessofchangingtheciphertexttotheplaintextthatprocessisknownas**decryption**.

PublicKeyEncryption: Asymmetric isaformofCryptosysteminwhichencryptionanddecryptionareperformedusingdifferentkeys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption.**

DifferencebetweenEncryptionandPublic-keyEncryption:

basis	**Encryption**	**Public-KeyEncryption**
RequiredforWork:	● Samealgorithmwiththesamekeyisusedforencryptionanddecryption. ● Thesenderandreceivermustsharethe algorithm and key.	● One algorithm is used for encryption andarelated algorithm decryption with pairofkeys, one for encryption and otherfordecryption. ● Receiver and Sender must each have oneofthe matched pair of keys (not identical) .
RequiredforSecurity:	● Keymustbekeptsecret. ● If the key is secret, it isveryimpossible to deciphermessage. ● Knowledge of the algorithmplussamples of ciphertext mustbeimpractical todeterminethekey.	● Oneofthetwokeysmustbekeptsecret. ● If one of the key is kept secret, it isveryimpossible to decipher message. ● Knowledge of the algorithm plus one ofthekeys plus samples of ciphertext mustbeimpractical to determine the other key.

CharacteristicsofPublicEncryptionkey:

- PublickeyEncryptionisimportantbecauseitisinfeasibletodeterminethedecryptionkeygivenonlytheknowledgeof the cryptographic algorithm and encryption key.
- Eitherofthetwokeys(PublicandPrivatekey)canbeusedforencryptionwithotherkeyusedfordecryption.
- Due to Public key cryptosystem, public keys can be freely shared,allowing users an easy and convenient methodforencrypting content and verifying digitalsignatures, and private keys can be kept secret, ensuringonly the ownersofthe private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem isRSA (Rivest–Shamir–Adleman). The difficulty of finding theprimefactors of a composite number is the backbone of RSA.

Example:

Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encryptthemessage using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No otherrecipientother than C can decrypt the message because only C know C's private key.

ryptographyanditsTypes

- Read
- Discuss
- Courses

Cryptographyistechniqueofsecuringinformationandcommunicationsthroughuseofcodessothatonlythosepersonforwhomtheinformation is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt”means“hidden” and suffix “graphy” means “writing”. In Cryptography the techniques which are use to protect informationareobtainedfrommathematicalconceptsandasetofrulebasedcalculationsknownasalgorithmstoconvertmessagesinwaysthat makeithard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect dataprivacy,web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today’s age of computers cryptography is often associated with the process whereanordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode itandhence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

FeaturesOfCryptographyareasfollows:

1. **Confidentiality:**Informationcanonlybeaccessedbythepersonforwhomitisintendedandnootherpersonexcepthimcanaccessit.
2. **Integrity:**Informationcannotbemodifiedinstorageortransitionbetweensenderandintendedreceiverwithoutanyaddition to information being detected.
3. **Non-repudiation:**Thecreator/senderofinformationcannotdenyhisintentiontosendinformationatlaterstage.
4. **Authentication:**Theidentitiesofsender andreceiverareconfirmed.Aswellasdestination/originofinformationisconfirmed.

TypesOfCryptography: Ingeneraltherearethreetypesofcryptography:

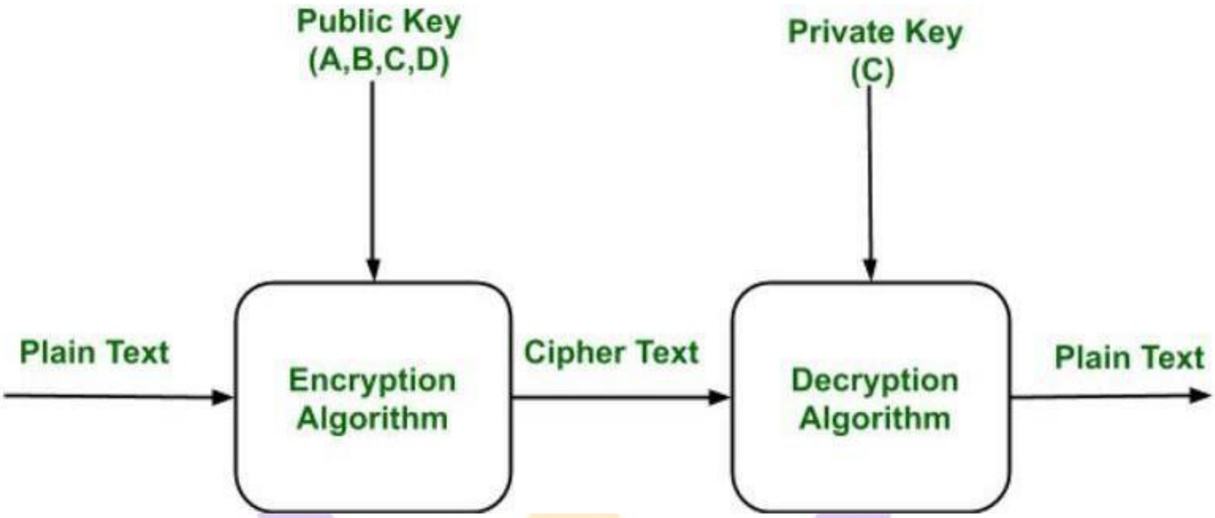
1. **SymmetricKeyCryptography:**Itisanencryptionsystemwherethesenderandreceiverofmessageuseasinglecommonkeytoencryptanddecryptmessages.SymmetricKeySystemsarefasterandsimplerbuttheproblemisthatsenderandreceiverhavetosomehowexchangekeyinasecuremanner.Themostpopularsymmetrickeycryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).
2. **HashFunctions:** Thereisnousageofanykeyinthisalgorithm.Ahashvaluewithfixedlengthiscalculatedaspertheplain textwhich makes it impossible for contents of plain text to be recovered. Many operating systems use hashfunctions toencryptpasswords.
3. **Asymmetric Key Cryptography:**Under this system a pair of keys is used to encrypt and decrypt information.Areceiver’spublickeyisusedforencryptionanda receiver’sprivatekeyis usedfor decryption.Public keyandPrivateKeyaredifferent. Even if the public key is knownby everyone the intended receiver canonly decode it because healoneknow his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

ApplicationsOfCryptography:

1. **Computerpasswords:**Cryptographyiswidelyutilizedincomputersecurity,particularlywhencreatingandmaintainingpasswords.Whenauserlogsin,theirpasswordishashedandcomparedtothehashthatwaspreviouslystored.Passwordsarehashedandencryptedbeforebeingstored.Inthistechnique, the passwords are encrypted sothat even if a hacker gains access to the password database, they cannotread the passwords.
2. **Digital Currencies:**To safeguard transactions and prevent fraud, digital currencies like Bitcoin alsousecryptography.Complexalgorithmsandcryptographickeysareusedtosafeguardtransactions,makingitnearlyhard totamper with or forge the transactions.
3. **Securewebbrowsing:**Onlinebrowsingsecurityisprovidedbytheuseofcryptography,whichshieldsusersfromeavesdropping andman-in-the-middle assaults. Publickey cryptographyis usedby theSecureSockets Layer(SSL)andTransportLayerSecurity(TLS)protocolstoencryptdatasentbetweenthewebserverandtheclient,establishingasecure channel for communication.
4. **Electronicsignatures:**Electronic signatures serveasthe digitalequivalentofa handwritten signatureand are usedtosign documents. Digital signatures are created using cryptography and can be validated using publickeycryptography. In many nations, electronic signatures are enforceableby law, andtheir use is expanding quickly.
5. **Authentication:**Cryptographyisusedforauthenticationinmanydifferentsituations,suchaswhenaccessingabankaccount,loggingintoacomputer,orusingasecurenetwork.Cryptographicmethodsareemployedbyauthenticationprotocolstoconfirmtheuser’sidentity and confirm that they have the required access rights to the resource.
6. **Cryptocurrencies:**Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum tosafeguardtransactions,thwartfraud,andmaintainthenetwork’sintegrity.Complexalgorithmsandcryptographickeysareusedto safeguard transactions, making it nearly hard to tamper with or forge the transactions.
7. **End-to-End Encryption:** End-to-end encryption is used to protect two-way communications likevideoconversations, instant messages, and email. Even if the message is encrypted, it assures that only theintendedreceivers can read the message.End-to-end encryption is widely used in communication apps likeWhatsApp andSignal, and it provides a high level of security and privacy for users.

Advantages

1. **AccessControl:**Cryptographycanbeusedforaccesscontroltoensurethatonlypartieswiththeproperpermissionshaveaccess to a resource. Only those with the correct decryption key can access the resource thanks to encryption.
2. **SecureCommunication:**Forsecure onlinecommunication,cryptography iscrucial.Itofferssecuremechanismsfortransmittingprivateinformationlikepasswords,bankaccountnumbers,andothersensitivedataovertheinternet.
3. **Protectionagainstattacks:**Cryptographyaidsinthedefenceagainstvarioustypesofassaults,includingreplayandman-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4. **Compliancewithlegalrequirements:**Cryptographycanassistfirmsinmeetingavarietyoflegalrequirements,including data protection and privacy legi



ComponentsofPublicKeyEncryption:

- **PlainText:** Thisisthemessagewhichisreadableorunderstandable.ThismessageisgiventotheEncryptionalgorithmasaninput.
- **CipherText:** TheciphertextisproducedasanoutputofEncryptionalgorithm.Wecannotsimplyunderstandthismessage.
- **EncryptionAlgorithm:** Theencryptionalgorithmisusedtoconvertplaintextintociphertext.
- **DecryptionAlgorithm:** Itacceptstheciphertextasinputandthematchingkey(PrivateKeyorPublickey)andproducestheoriginalplaintext
- **PublicandPrivateKey:** OnekeyeitherPrivatekey(Secretkey)orPublicKey(knowntoeveryone)isusedforencryptionandotherisusedfordecryption

WeaknessofthePublicKeyEncryption:

- PublickeyEncryptionisvulnerabletoBrute-forceattack.
- Thisalgorithmalsofailswhentheuserlosthisprivatekey,thenthePublickeyEncryptionbecomesthemostvulnerablealgorithm.
- PublicKeyEncryptionalsoisweaktowardsmaninthemiddleattack.Inthisattackathirdpartycandisruptthepublickeycommunication and then modify the public keys.
- If user private key used for certificate creation higher in the PKI(Public Key Infrastructure) server hierarchyiscompromised, or accidentally disclosed, then a "man-in-the-middle attack" is also possible, making anysubordinatecertificate wholly insecure. This is also the weakness of public key Encryption.

ApplicationsofthePublicKeyEncryption:

- **Encryption/Decryption:** ConfidentialitycanbeachievedusingPublicKeyEncryption.InthisthePlaintextisencryptedusingreceiverpublickey. This will ensure that no one other than receiver private key can decrypt the cipher text.
- **Digital signature:** Digitalsignatureisforsendersauthenticationpurpose.Inthissenderencrypttheplaintextusinghisownprivatekey.Thisstepwillmake suretheauthenticationofthesenderbecausereceivercandecrypttheciphertextusingsenderspublickeyonly.
- **Keyexchange:** ThisalgorithmcanuseinbothKey-managementandsecurelytransmissionofdata.

PublicandprivateCryptographyanditsTypes:

Cryptographyistechnique of securing information and communications through use of codes so that only those person for whomtheinformationis intendedcanunderstandit and processit.Thuspreventing unauthorizedaccessto information. Theprefix "crypt"means"hidden" and suffix "graphy" means "writing".In Cryptography the techniques which are use to protect information are obtainedfrommathematicalconceptsandasetofrulebasedcalculationsknownasalgorithmstoconvertmessagesinwaysthatmakeithardtodecode it.Thesealgorithmsare usedfor cryptographic key generation, digital signing, verificationto protect data privacy,webbrowsingoninternet and toprotect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today'sage of computers cryptography is often associated with the process where anordinaryplaintextisconvertedtociphertext whichisthetext madesuchthatintendedreceiverofthetext canonlydecodeitandhencethisprocess is knownasencryption. The process ofconversion of cipher text to plain text this is known as decryption.

FeaturesOfCryptographyareasfollows:

1. **Confidentiality:**Information canonlybeaccessedbythepersonfor whomitisintendedandnootherpersonexcepthim can access it.
2. **Integrity:**Informationcannotbemodifiedinstorageortransitionbetweensenderandintendedreceiver withoutanyaddition to information being detected.

3. **Non-repudiation:**Thecreator/senderofinformationcannotdenyhisintentiontosendinformationatlaterstage.
4. **Authentication:**Theidentitiesofsenderandreceiver areconfirmed.As wellasdestination/originofinformationisconfirmed.

TypesOfCryptography: IngeneraltherearethreetypesOfcryptography:

1. **SymmetricKeyCryptography:** Itisanencryptionsystemwherethesenderandreceiver of messageusea singlecommonkey to encrypt and decrypt messages. Symmetric Key Systemsare faster and simpler but the problem isthatsender andreceiver have to somehow exchange key in a secure manner. The most popularsymmetric key cryptographysystem areData Encryption System(DES) and Advanced Encryption System(AES).
2. **Hash Functions:** There is nousage ofany keyin this algorithm. A hash value with fixedlength is calculated as pertheplaintextwhichmakesitimpossibleforcontentsofplaintexttoberecovered.Manyoperating systemsusehashfunctionsto encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information.Areceiver's public key isused for encryption and a receiver's private key is used for decryption. Public key andPrivateKeyaredifferent.Evenifthepublickeyisknownbyeveryonetheintendedreceiver canonlydecodeit becausehealone know his private key. The most popular asymmetrickey cryptography algorithm is RSA algorithm.

ApplicationsOfCryptography:

1. **Computerpasswords:**Cryptography iswidely utilizedincomputersecurity, particularly whencreating andmaintainingpasswords. Whena user logs in,their password is hashedandcompared tothe hash that was previouslystored.Passwordsarehashedandencryptedbeforebeingstored.Inthistechnique,thepasswordsareencrypted sothatevenifahacker gainsaccess to the password database, they cannot read the passwords.
2. **Digital Currencies:** To safeguard transactions and prevent fraud, digital currencies like Bitcoin also usecryptography.Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard totamper with orforge the transactions.
3. **Secure web browsing:** Online browsing security is provided by the use of cryptography, which shieldsusersfromeavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL)andTransportLayerSecurity(TLS)protocolstoencryptdatasentbetweenthewebserverandtheclient,establishingasecurechannelfor communication.
4. **Electronic signatures:** Electronic signatures serve asthe digital equivalent ofa handwritten signatureand are usedtosigndocuments.Digitalsignaturesarecreatedusingcryptographyandcanbevalidatedusingpublickeycryptography. Inmany nations, electronic signatures are enforceable by law, and their use is expanding quickly.
5. **Authentication:** Cryptography is used for authentication in many different situations, such as when accessing abankaccount, logging into a computer, or using a secure network. Cryptographic methodsare employed byauthenticationprotocolstoconfirmtheuser'sidentityandconfirmthat theyhavetherequiredaccessrightstotheresource.
6. **Cryptocurrencies:**CryptographyisheavilyusedbycryptocurrencieslikeBitcoinandEthereumtosafeguard transactions,thwart fraud,and maintainthenetwork'sintegrity.Complexalgorithmsandcryptographickeysareusedtosafeguard transactions, making it nearly hard to tamper with or forge the transactions.
7. **End-to-End Encryption:** End-to-end encryption is used to protect two-way communications like videoconversations,instant messages,and email.Evenifthemessage isencrypted,itassuresthatonlytheintendedreceiverscanread themessage.End-to-endencryptioniswidelyusedin communicationappslikeWhatsAppandSignal,and it providesahighlevel of security and privacy for users.

Advantages

1. **Access Control:** Cryptography can be used for access control to ensure that only parties with the properpermissionshaveaccesstoaresource.Onlythosewiththecorrect decryptionkeycanaccesstheresourcethankstoencryption.
2. **SecureCommunication:** For secureonlinecommunication, cryptography iscrucial. It offerssecure mechanismsfortransmittingprivateinformationlikepasswords,bankaccountnumbers,andothersensitivedataovertheinternet.
3. **Protectionagainst attacks:** Cryptographyaidsinthedefenceagainst varioustypesofassaults,includingreplayandman-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4. **Compliance withlegalrequirements:**Cryptographycanassist firmsinmeetinga varietyoflegalrequirements,including data protection and privacy legislation.

ElectronicGovernance:

Cybersecurityisacriticalpartofprotectingbusinessandindividualdata.It'sessentialtohaveagovernanceplaninplacethatoutlineshow yourorganizationwillrespondtocyberattacks.Failuretodosocanleadtoseriousconsequences,suchasfinanciallosses,databreaches, and even legal ramifications.

Whatissecuritygovernance?

Governance in cybersecurity refers to the overall process and systems that are in place to ensure the security of anorganization'sdigitalassetsand infrastructure.This includes establishing policies, procedures, andstandards forhowinformationisprotected,identifyingandmitigatingthreats, ensuringcompliancewith regulatoryrequirements, andmonitoringandmanagingrisk.

Thereareanumberofdifferenttypesofgovernancemodelsthatcanbedeployedincybersecurity,includingcentralized,distributed,semi-centralized,andself-organizing.Eachhasitsownadvantagesanddisadvantages,soit'simportanttochoosethemodelthatbestsuitsyourorganization'sneeds.

Centralized governancemodelsinvolveasinglepointofcontrolandauthorityoverallaspectsofcybersecurity.Thistypeof modelistypicallyused by large organizations withcomplex security structures andlots of resources available to implement robust controls.However,centralized governance models can be difficult to scale up or adapt when threats change or new technologies emerge.

Distributedgovernancemodelsrelyonanetworkofinterconnectednodestomanagesecurityresourcesanddata.Thistypeofmodelispopular among small businessesthat don’t have the resources or need for acentralized system. However, distributed models canbeless effective at detecting attacks early enough or tracking malicious actors across multiple sites.

TypesofCybersecurityGovernance

Cybersecurity governance is the process of allocating resources, setting policies and procedures, and implementing actionstomaintain situational awareness and protect systems and information from cyber threats. Cybersecurity governance can bedividedinto five types: operational, technical, management, legal, and policy.

Operationalcybersecuritygovernanceisresponsibleforensuringthattheorganization'snetworksareoperationalandthatemployeesarefollowingestablishedprotocols.Technicalcybersecuritygovernancedetermineshowdevicesareconfigured,monitored,andsecured.Managementcybersecuritygovernanceensuresthattheorganizationhasaplaninplacetomanagecyberrisk,assignsresponsibilitiesandmanagesaccountability.Legalcybersecuritygovernanceincludesunderstandingapplicablelawsandregulationsrelatedtocybersecurity,aswellasappointingalawyertoadviseoncybersecurityissues.Policycybersecuritygovernanceestablishes guidelines for acceptable behaviorincyberspace.Eachtype of cybersecurity governance has its ownsetof goals,objectives, andprocesses.

One of the most important aspectsof cybersecurity governance is establishing aneffective chain ofcommunicationbetweenvariousparts of the organization. This allows for closer monitoring of activities and faster identification of problems. Cybersecurityteamsshould also have access to information about all systems within the organization so that they can quickly identify potentialthreats.

PrinciplesofCybersecurityGovernance

Governanceincybersecurityistheprocessofassigningandmanagingresponsibilities formanaginganorganization's cybersecurityposture. Governance should be aligned with the organization's risk management framework and should provide aframework formaking decisions about cyber security policies and activities.

Agoodgovernanceframeworkwillinclude:

- *–Cybersecurityriskassessment*
- *–Identificationofcriticalassetsandsystems*
- *–Establishmentofbaselinecybersecuritycontrols*
- *–Authorizationofactivitiesrelatedtocriticalassetsandsystems*
- *–Monitoringandevaluationofcompliancewithbaselinecybersecuritycontrols*

ImplementationofCybersecurityGovernance

Cybersecuritygovernanceistheprocessandsystemforgoverningthecybersecurityofanorganization.Itencompassesallaspectsoforganizational security, from risk management to incident response and prevention. Cybersecurity governance should beimplemented atevery level of an organization, from the board of directors to the individual employee.

Thereareseveralkeyelementsofcybersecuritygovernance,including:

- ***Riskassessment:****Identifyingandassessingpotentialcyberthreatsandvulnerabilities.*
- ***Organizationaldesign:****Ensuringthatorganizationalstructures andcapabilitiesareinplacetorespondtoincidentsquicklyandeffectively.*
- ***Incidentresponse:****Planningandexecutingthenecessarystepstoprotectagainst,detect,andrespondtoincidents.*
- ***Prevention:****Implementingbestpracticesandpoliciestoreducethelikelihoodofincidentshappeninginthefirstplace.*

Whatdoesagoodapproachtosecuritygovernancelooklike?

Thisisadifficultquestiontoanswer,asgovernanceincybersecurityisaconstantlyevolvingandcomplexproblem.Inthisblogpost,wewilldiscuss some of the key considerations when designing or implementing a governance framework for cyber security.

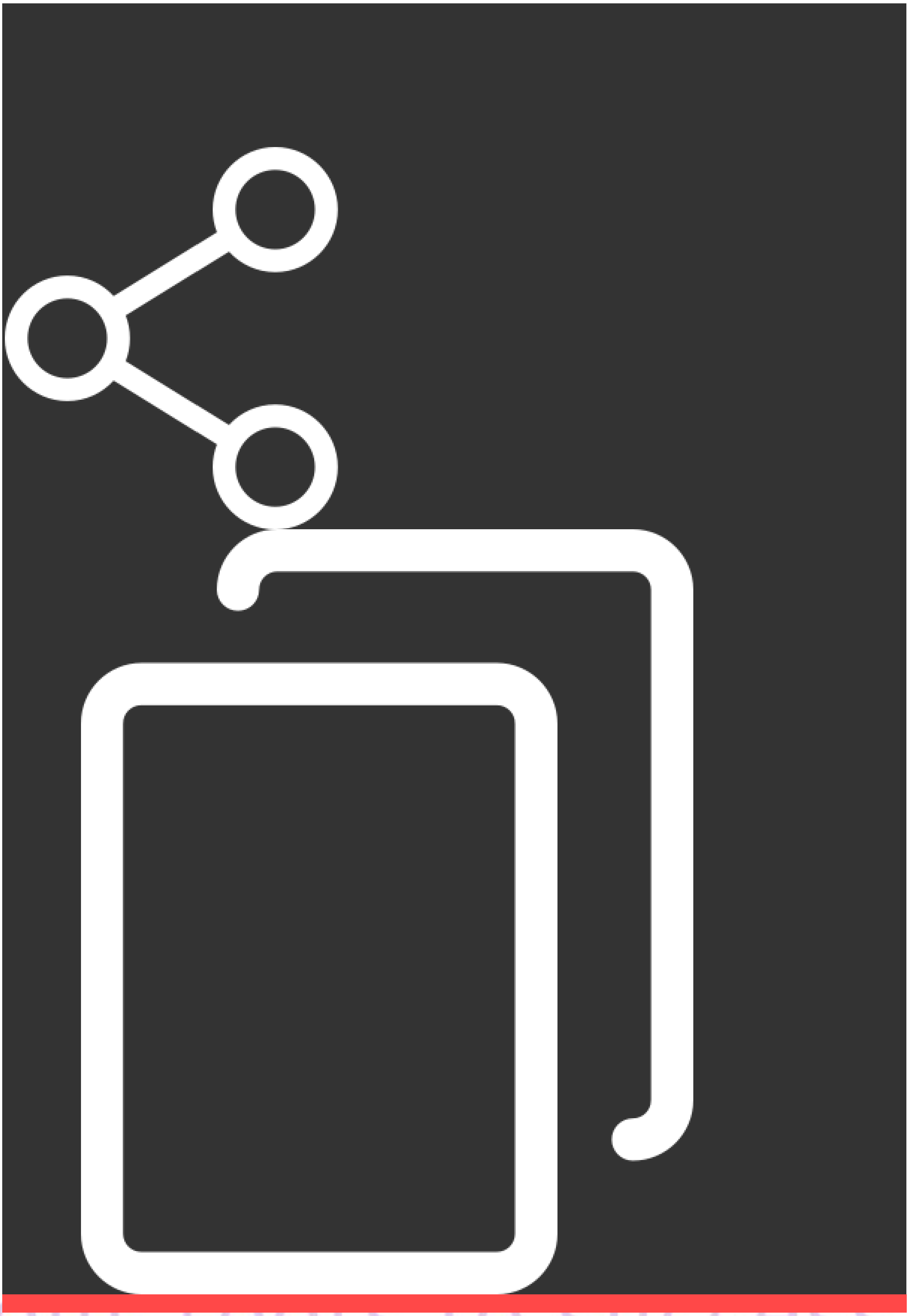
First, it is important to understand the purpose ofgovernance in cybersecurity. Governance can help to ensure that systemsareproperlyconfiguredandoperated, thatriskassessmentsareaccurate,andthatproper decision-makingprocessesareinplace.

Second, thereare different types ofcybersecurity governanceframeworks. Some frameworks focus onoverallsystemmanagement,whileothersemphasizemorespecificareassuchasinformation security orincidentresponse.Itisimportanttochooseaframeworkthat suits the needs of the organization and its employees.

Third,it is essential tohaveaneffectivecommunicationandcollaborationframeworkinplace.A goodgovernance systemshouldallow for sharing of information between stakeholders, as well as cooperation during incidents.

Overall,agoodapproachtosecuritygovernanceinvolvesthoughtfulplanningandconstantevaluation.

LigalRecognizationElectronicRecords:



CyberLaws

According to the definition of E-governance provided by the World Bank, it is the approach of governmental agencies to use technologies related to communication and information for the purpose of transforming and strengthening relations with businesses, citizens, and other governmental agencies. The IT Act, 2000, defines one of its prime objectives as electronic governance or e-governance promotion. Let us discuss electronic records and E-governance in detail.

Mentionofe-GovernanceandAssociatedProvisionsintheITAct,2000

Toknowwhatane-recordis,itisimportanttounderstandtheelectronicrecord'smeaning.Theelectronicrecordmeaningisbest describedinthelegalrecognitionofelectronicrecords,digitalsignatures,andassociatedtopics,forwhichthefollowingprovisionsofthe IT Act, 2000 were formulated.

- **LegalRecognitionofElectronicRecords(MentionedinSection4oftheAct)**

  Foranyimportantpointtobecomealaw,itisneededtobewritten,printed,ortypewritten.Itcanalsobeconsideredto be a law if the information is provided in an electronic form. However, the electronic form must be accessible all the time for subsequent referencing.

- **LegalRecognitionofSignatures(MentionedinSection5oftheAct)**

  Mostofthedocumentsrelatedtoapersonareauthenticatedbyhisorhersignature.Ifthepersoncanproduceadigital formofhissignatureacceptablebythecentralgovernment,thenthepersonislegallyallowedtovalidatethedocuments withthe digital signature. This is the summary of the legal recognition of digital signature provision.

- **ApplicationofDigitalSignatureandElectronicRecordsinGovernmentanditsAgencies(MentionedinSection6of the Act)**

  Accordingtothisprovision,ifthelawallowsaperson

- Tofillanapplication,form,ordocumentrelatedtoGovernmentauthoritiesorrelatedagencies,

- Toissueorgrantsanction,licence,approval,orpermitinaparticularway,

- ToPayorreceivemoneyinacertainmannerthenthepersoncancertainlydosoinanelectronicformifhemaintainsthe government-approvedformat.

Additionally,themannerandformatofcreating,issuing,andfilingelectronicrecords,andthemethodsofpaymentoffeesforthesamemay beprescribed.

- **RetentionofElectronicRecords(MentionedinSection7oftheAct)**

  The law can alsoretain the electronic form of any information, document, or record if it needs to do so. Retention of records can take place if the records are accessible and available for subsequent referencing, the format of the informationisunchanged,oraccuratelyrepresenttheoriginalinformation,andadequateinformationofthedestination, origin, and date and time of receipt or dispatch of the record. The law does not hold for automatically generated informationrelatedtothedispatchorreceiptoftherecord.However,theprovisiondoesnotapplytolawsthatexpressly provide for electronic retention of documents, records, and information.

- **PublicationsofrulesandregulationsinElectronicGazette(mentionedinSection8oftheAct)**

  Ifthelawrequirestopublishanyofficialrule,regulation,notification,by-lawandrelatedmattersintheOfficialGazette, thenitcanalsodosointheElectronicGazette.Thepublicationdateofsuchrulesandregulationswillbethesameasitsfirst published date in any form of the Gazette.

- **Section6,7,and8doesnotProvidetheRighttoinsistAcceptanceofanElectronicFormofthe Document(Mentioned in Section 9 of the Act)**

  Theprevioussections 6,7,and8donot granttherighttoanypersontoinsistontheissuance,acceptance, retention, orcreationofanydocumentormonetarytransactionsdirectlyfrom thecentral orthestategovernment,ministryofthe department, or associated agencies.

- **ProvidePowertotheCentralGovernmenttoMakeRulesforLegalRecognitionofDigitalSignatures(Mentionedin Section 10 of the Act)**

AccordingtotheITAct,2000,thecentralgovernmenthasthepowertoprescribe:

- Formatandmannerofaffixationofthedigitalsignature.

- Digitalsignaturetype.

- Identificationprocedureforthepersonwhoaffixesthedigitalsignature.

- Determinestheprocedurestojustifythesecurity,integrity,andconfidentialityofelectronicrecords.

- Anyotherlegalproceduresfordigitalsignature.

DataProtection

AccordingtoSection43AoftheITAct,2000,ifthebodyresponsibleformaintainingthesecurityofpersonalinformationanddata in a computer resource shows negligence leading to wrongful gain or loss, then the body is liable for paying damages as compensationupto5crorerupees.Additionally,theGovernmentofIndiaincorporatedtheInformationTechnologyRules,2011, under section43A of theIT Act, 2000, which applies therules of securityto all corporatebodies in India.

LegalRecognitionofDigitalSignatureCertifyingAuthorities:

Section1:ShortTitle,Extent,CommencementandApplication

(1) ThisActmaybecalledtheInformationTechnologyAct,2000.

(2) Itshallextendtothewholeof Indiaand,saveasotherwiseprovidedinthisAct,itappliesalsotoanyoffence or contravention thereunder committed outside India by any person.

(3) It shall come into force on suchdate as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) NothinginthisActshallapplytodocumentsortransactionsspecifiedintheFirstSchedulebywayofadditionordeletion of entries thereto.

(5) Everynotificationissuedundersub-section(4)shallbelaidbeforeeachHouseofParliament.

Secton2:Definition

(1) InthisAct,unlessthecontextotherwiserequires,

(a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicatingwiththelogical,arithmetical,or memoryfunctionresourcesof acomputer,computersystemor computer network;

(b) "Addressee"meansapersonwhoisintendedbytheoriginatortoreceivetheelectronicrecordbutdoesnot includeany intermediary;

(c) "AdjudicatingOfficer"meansadjudicatingofficerappointedundersubsection(1)ofsection46;

(d) "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;

(e) "AppropriateGovernment"meansasrespectsanymatter:

(i) enumeratedinListIIoftheSeventhScheduletotheConstitution;
(ii) relatingtoanyStatelawenactedunderListIIIoftheSeventhScheduletotheConstitution,theState Government and in any other case, the Central Government;

(f) "AsymmetricCryptoSystem"meansasystemofasecurekeypairconsistingofaprivatekeyforcreatinga digitalsignatureandapublickeytoverifythedigitalsignature;

(g) "CertifyingAuthority"meansapersonwhohasbeengrantedalicencetoissueaElectronicSignature Certificate under section 24;

(h) "CertificationPracticeStatement"meansastatementissuedbyaCertifyingAuthoritytospecifythepractices thattheCertifyingAuthorityemploysinissuingElectronicSignatureCertificates;

(ha)"CommunicationDevice"meanscellphones,personaldigitalassistance,orcombinationofbothoranyother deviceusedtocommunicate,sendortransmitanytext,video,audio,orimage.

(i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) “ComputerNetwork”meanstheinterconnectionofoneormorecomputersorcomputersystemsor Communicationdevicethrough-

(i) theuseofsatellite,microwave,terrestrialline,wire,wirelessorothercommunicationmedia;and
(ii) terminalsoracomplexconsistingoftwoormoreinterconnectedcomputersorcommunicationdevicewhetherornot the interconnection is continuously maintained;

(k) “ComputerResource”meanscomputer,communicationdevice,computersystem,computernetwork,data, computerdatabaseorsoftware;

(l) “Computer System” means a device or collection of devices, including input and output support devices and excluding calculatorswhich are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) “Controller”meanstheControllerofCertifyingAuthoritiesappointedundersub-section(7)ofsection17;

(n) “Cyber Appellate Tribunal” means theCyber Appellate Tribunal established under sub-section (1)ofsection 48;

(na)“Cybercafe”meansanyfacilityfromwhereaccesstotheinternetisofferedbyanypersonintheordinary courseofbusinesstothemembersofthepublic.

(nb) “Cyber Security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored threin from unauthorized access, use, disclosure, disruption, modification or destruction.

(o) “Data” means a representation of information, knowledge, facts, concepts or instructions which are being preparedorhavebeenpreparedinaformalisedmanner,and isintendedtobeprocessed,isbeingprocessedor has beenprocessed in acomputer systemor computer network. ,.and maybe in any form (including computer printoutsmagneticoropticalstorage media,punchedcards, punchedtapes)or storedinternally in thememory of the computer;

(p) “DigitalSignature”meansauthenticationofanyelectronicrecordbyasubscriberbymeansofanelectronic methodorprocedureinaccordancewiththeprovisionsofsection3;

(q) “Digital Signature Certificate” means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) “ElectronicForm”withreferencetoinformationmeansanyinformationgenerated,sent,receivedorstoredin media,magnetic,optical,computermemory,microfilm,computergeneratedmicroficheorsimilardevice;

(s) “ElectronicGazette”meansofficialGazettepublishedintheelectronicform;

(t) “Electronic Record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(ta)“ElectronicSignature”meansauthenticationofanyelectronicrecordbyasubscriberbymeansofthe electronictechniquespecifiedinthesecondscheduleandincludesdigitalsignature

(tb) “Electronic Signature Certificate” means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate”

(u) “Function”, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua)“IndianComputerEmergencyResponseteam”meansanagencyestablishedundersub-section(1)ofsection70B

(v) “Information” includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

(w) “Intermediary”withrespecttoanyparticularelectronicrecords,meansanypersonwhoonbehalfofanother personreceives,storesortransmitsthatrecordorprovidesanyservicewithrespecttothatrecordandincludes telecomserviceproviders,networkserviceproviders,internetserviceproviders,webhostingserviceproviders, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

(x) “KeyPair”,inanasymmetriccryptosystem,meansaprivatekeyanditsmathematicallyrelatedpublickey, whicharesorelatedthatthepublickeycanverifyadigitalsignaturecreatedby theprivatekey;

(y) “Law” includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or aGovernor,asthecasemaybe.RegulationsmadebythePresidentunderarticle240,BillsenactedasPresident’s Actundersub-clause(a)ofclause(1)ofarticle357oftheConstitutionandincludesrules,regulations,bye-laws and orders issued or made thereunder;

(z) “Licence”meansalicencegrantedtoaCertifyingAuthorityundersection24;

(za) “Originator” means a person who sends, generates, stores or transmits any electronic message or causes anyelectronicmessagetobesent,generated,storedortransmittedtoanyotherpersonbutdoesnotincludeanintermediary ;

(zb)“Prescribed”meansprescribedbyrulesmadeunderthisAct;

(zc)“PrivateKey”meansthekeyofakeypairusedtocreateadigitalsignature;

(zd)“PublicKey”meansthekeyofakeypairusedtoverifyadigitalsignatureandlistedintheDigitalSignature Certificate;

(ze)“SecureSystem”meanscomputerhardware,software,andprocedurethat-:

(a) are reasonably secure from unauthorised access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adheretogenerallyacceptedsecurityprocedures;

(zf)“SecurityProcedure”meansthesecurityprocedureprescribedundersection16bytheCentralGovernment;

(zg)“Subscriber”meansapersoninwhosenametheElectronicSignatureCertificateisissued;

(zh)“Verify”inrelationtoadigitalsignature,electronicrecordorpublickey,withitsgrammaticalvariationsand cognateexpressionsmeanstodeterminewhether

(a) the initial electronic record was affixed with the digital signature by the use ofprivate keycorresponding to the public key of the subscriber;
(b) theinitialelectronicrecordisretainedintactorhasbeenalteredsincesuchelectronicrecordwassoaffixedwith the digital signature.

(2) AnyreferenceinthisActtoanyenactmentoranyprovisionthereofshall,inrelationtoanareainwhichsuch enactmentorsuchprovisionisnotinforce,beconstruedasareferencetothecorrespondinglawortherelevant provision of the corresponding law, if any, in force in that area.

Section3:AuthenticationofElectronicRecords

(1) Subjecttotheprovisionsofthissectionanysubscribermayauthenticateanelectronicrecordbyaffixinghis Digital Signature.

(2) The authentication of the electronic record shall be effectedby the use of asymmetriccrypto system andhashfunctionwhichenvelopandtransformtheinitialelectronicrecordintoanotherelectronicrecord.

Explanation –
Forthepurposesofthissub-section,"Hashfunction"meansanalgorithmmappingortranslationofonesequence ofbitsintoanother,generallysmaller,setknownas"HashResult"suchthatanelectronicrecordyieldsthesame hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) toderiveorreconstructtheoriginalelectronicrecordfromthehashresultproducedbythealgorithm;
(b) thattwoelectronicrecordscanproducethesamehashresultusingthealgorithm.

(3) Anypersonbytheuseofapublickeyofthesubscribercanverifytheelectronicrecord.

(4) Theprivatekeyandthepublickeyareuniquetothesubscriberandconstituteafunctioningkeypair.

Section3A:ElectronicSignature

(1) Notwithstandinganythingcontainedinsection3,butsubjecttotheprovisionsofsub-section(2),asubscriber mayauthenticateanyelctronicrecordbysuchelectronicsignatureorelectronicauthenticationtechniquewhich-

(a) isconsideredreliable;and

(b) maybespecifiedintheSecondSchedule

(2) Forthepurposesofthissectionanyelectronicsignatureorelectronicauthenticationtechniqueshallbeconsidered reliable if-

(a) thesignaturecreationdataortheauthenticationdataare,withinthecontextinwhichtheyareused,linked to the signatoryor ,as the casemaybe,the authenticator and of no otherperson;
(b) the signature creation data or the authentication data were, at the time of signing, under thecontrol of the signatory or, as the case may be,the authenticator and of no other person;
(c) anyalterationtotheelectronicsignaturemadeafteraffixingsuchsignatureisdetectable
(d) anyalterationtotheinformationmadeafteritsauthenticationbyelectronicsignatureisdetectable;and
(e) itfulfillssuchotherconditionswhichmaybeprescribed.

(3) TheCentralGovernmentmayprescribetheprocedureforthepurposeofascertainingwhether

electronicsignatureisthatofthepersonbywhomitispurportedtohavebeenaffixedorauthenticated.

(4) TheCentralGovernemntmay,bynotificationintheOfficialGazette,addtoor omitany electronic signature or electronicauthenticationtechniqueandtheprocedureforaffixingsuchsignaturefromthesecondschedule;

Providedthatnoelectronicsignatureorauthenticatontechniqueshallbespecifiedinthe SecondScheduleunless such signature or technique is reliable.

(5) Everynotificationissuedundersub-section(4)shallbelaidbeforeeachHouseofParliament.

Chapter3:ElectronicGovernance

LeaveaComment

Section4:LegalRecognitionofElectronicRecords

Section5:LegalrecognitionofElectronicSignature

Section6:UseofElectronicRecordsandElectronicSignatureinGovernmentanditsagencies

Section6A:DeliveryofServicesbyServiceProvider

Section7:RetentionofElectronicRecords

Section7A:AuditofDocumentsetcinElectronicform

Section8:Publicationofrules,regulation,etc,inElectronicGazette

Section9:Sections6,7and8NottoConferRighttoinsistdocumentshouldbeacceptedinelectronicform

Section10:PowertoMakeRulesbyCentralGovernmentinrespectofElectronicSignature

Section10A:Validityofcontractsformedthroughelectronicmeans

Section4:LegalRecognitionofElectronicRecords

Whereanylawprovidesthatinformationoranyothermatter shallbeinwritingorinthetypewrittenorprintedform, then, notwithstanding anything contained in such law, such requirement shall be deemed to have beensatisfied if such information or matter is

(a) renderedormadeavailableinanelectronicform;and

(b) accessiblesoastobeusableforasubsequentreference

Section5:LegalrecognitionofElectronicSignature

Whereanylawprovidesthatinformationor anyother mattershallbeauthenticated byaffixingthesignatureor anydocumentshouldbesignedorbearthesignatureofanypersonthen,notwithstandinganythingcontainedin suchlaw,suchrequirementshallbedeemedtohavebeensatisfied,ifsuchinformationormatterisauthenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Explanation –
For the purposes of this section, “Signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression “Signature” shall be construed accordingly.

Section6:UseofElectronicRecordsandElectronicSignatureinGovernmentanditsagencies

(1) Whereanylawprovidesfor

(a) the filing of any form, application or any other document with any office, authority, body or agency owned orcontrolledbytheappropriateGovernmentinaparticularmanner;
(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) TheappropriateGovernmentmay,forthepurposesofsub-section(1),byrules,prescribe–

(a) themannerandformatinwhichsuchelectronicrecordsshallbefiled,createdorissued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

Section6A:DeliveryofServicesbyServiceProvider

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation:Forthepurposesofthissection,serviceprovidersoauthorizedincludesanyindividual,private agency,privatecompany,partnershipfirm,soleproprietorformoranysuchotherbodyoragencywhichhas beengrantedpermissionbytheappropriateGovernmenttoofferservicesthroughelectronicmeansinaccordancewith the policy governing such service sector.

(2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subjecttotheprovisionsofsub-section(2),theappropriateGovernmentmayauthorizetheserviceproviders to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) TheappropriateGovernmentshall,bynotificationintheOfficialGazette,specifythescaleofservicecharges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

Section7:RetentionofElectronicRecords

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, –

(a) theinformationcontainedthereinremainsaccessiblesoastobeusableforasubsequentreference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a formatwhichcanbedemonstratedtorepresentaccuratelytheinformationoriginallygenerated,sentorreceived;

(c) thedetailswhichwillfacilitatetheidentificationoftheorigin,destination,dateandtimeofdispatchorreceipt of such electronic record are available in the electronic record:

Providedthat

thisclausedoesnotapplytoanyinformationwhichisautomaticallygeneratedsolelyforthepurposeofenabling an electronic record to be dispatched or received.

(2) Nothinginthissectionshallapplytoanylawthatexpresslyprovidesfortheretentionofdocuments,records or information in the form of electronic records. Publication of rules. regulation, etc.. in Electronic Gazette.

Section7A:AuditofDocumentsetcinElectronicform

Whereinanylawforthetimebeinginforce,thereisaprovisionforauditofdocuments,recordsorinformation, that provision shall also beapplicable for audit of documents, recordsor informationprocessed andmaintained in electronic form.

Section8:Publicationofrules,regulation,etc,inElectronicGazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Providedthat

whereany rule,regulation, order,bye-law,notificationor anyother matterspublishedinthe OfficialGazetteor ElectronicGazette,thedateofpublicationshallbedeemedtobethedateoftheGazettewhichwasfirstpublished in any form.

Section9:Sections6,7and8NottoConferRighttoinsistdocumentshouldbeacceptedinelectronicform

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain andpreserveanydocumentintheformofelectronicrecordsoreffectanymonetarytransactionintheelectronic form.

Section10:PowertoMakeRulesbyCentralGovernmentinrespectofElectronicSignature

TheCentralGovernmentmay,forthepurposesofthisAct,byrules,prescribe

(a) the type of Electronic Signature;
(b) the manner and format in which the Electronic Signature shall be affixed;
(c) themannerorprocedurewhichfacilitatesidentificationofthepersonaffixingtheElectronicSignature;
(d) controlprocessesandprocedurestoensureadequateintegrity,securityandconfidentialityofelectronicrecordsor payments; and
(e) anyothermatterwhichisnecessarytogivelegaleffecttoElectronicSignature.

Section10A:Validityofcontractsformedthroughelectronicmeans

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record,suchcontractshallnotbedeemedtobeunenforceablesolelyonthegroundthatsuchelectronicformormeanswas used for that purpose.

CyberCrimesOffenses&PenaltiesInIndia
IndiaInformationTechnologyActhasbeenprotectingcitizensfromwhite-collarcrimestoattacksbyterrorist

Thelaws forcybercrimesafeguardcitizens from dispensingcriticalinformation toastrangeronline.Theriseofthe21stcenturymarked theevolutionof cyberlaw in India with the **Information Technology Act, 2000.**

Mostofthecybercrimes–Hacking,Datatheft,IllegaltamperingwithsourcecodesarelistedundertheInformationTechnologyAct(ITAct),whichwasamendedin2008.TheActexplainsthetypesofcyber-crimeaswellastheassociatedpunishment.Thecompletetableisprovidedto createcyberawarenessamongthepeopleofIndia.

ITAct2000–Penalties,OffencesWithCaseStudies

June24,2014LionelFaleiroCaseStudies,Compliance,Laws&Regulations6

1. *ObjectivesofITlegislationinIndia*

TheGovernmentofIndiaenacteditsInformationTechnologyAct2000withtheobjectivesstatingofficiallyas:

"toprovidelegalrecognitionfortransactionscarriedoutbymeansofelectronicdatainterchangeandothermeansofelectroniccommunication,commonlyreferredtoas"electroniccommerce",whichinvolvetheuseofalternativestopaper-basedmethodsofcommunicationandstorageofinformation,tofacilitateelectronicfilingofdocumentswiththeGovernmentagenciesandfurthertoamendtheIndianPenalCode,theIndianEvidenceAct,1872,theBankers'BooksEvidenceAct,1891andtheReserveBankofIndiaAct,1934andformattersconnectedtherewithorincidentalthereto."

What does IT Act 2000 legislation deals with?
TheActessentiallydealswiththefollowingissues:

- LegalRecognitionofElectronicDocuments
- LegalRecognitionofDigitalSignatures
- OffensesandContraventions
- JusticeDispensationSystemsforcybercrimes.

Why did the needforIT AmendmentAct2008 (ITAA) arise?The ITAct 2000, beingthefirst legislation ontechnology, computers, e-commerce ande-communication,the wasthesubjectofextensivedebates,elaboratereviewswithonearmoftheindustrycriticizingsomesections of theAct to be draconian and other statingit is too diluted and lenient. There were some obvious omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian PenalCodeevenintechnologybasedcaseswiththeITActalsobeingreferredintheprocesswiththereliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act. Major industry bodies were consulted and advisory groups wereformed togointotheperceived lacunaeinthe I.T. Act andcomparingit with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrativeprocedures,theconsolidatedamendmentcalledthe**InformationTechnologyAmendmentAct2008**was placed in the Parliament and passed at the end of 2008 (just after Mumbai terrorist attack of 26 November 2008 had taken place). The IT Amendment Act 2008 gotthePresident assent on5 Feb 2009 and was made effective from 27 October 2009.

NotablefeaturesoftheITAA2008are:

- Focusingondataprivacy
- FocusingonInformationSecurity
- Definingcybercafé
- Makingdigitalsignaturetechnologyneutral
- Definingreasonablesecuritypracticestobefollowedbycorporate
- Redefiningtheroleofintermediaries
- RecognizingtheroleofIndianComputerEmergencyResponseTeam
- Inclusionofsomeadditionalcybercrimeslikechildpornographyandcyberterrorism
- AuthorizinganInspectortoinvestigatecyberoffenses(asagainsttheDSPearlier)

2. *StructureofITAct*

- **How is IT Act structured?**TheActtotallyhas13chaptersand90sections. Sections 91 to 94 deal with the amendments to the four Acts namely Indian Penal Code 1860, The Indian Evidence Act 1872,TheBankers'BooksEvidenceAct1891andtheReserveBankofIndiaAct1934.The Act has chapters that deal with authentication of electronic records, electronic signatures etc. Elaborate procedures for certifying authoritiesand electronic signatures have been spelt out.Thecivil offenceofdatatheftandtheprocessofadjudicationandappellateprocedures havebeendescribed.ThentheActgoesontodefineanddescribesomeofthewell-known cybercrimesandlaysdownthepunishmentstherefore.Thentheconceptofduediligence,roleof intermediaries and some miscellaneous provisions have been described.
- **What is the applicability of IT Act?**The Act extends to the whole of India and except as otherwise provided, it also applies to anyoffenceorcontraventionthereundercommittedoutsideIndiabyanyperson. RulesandproceduresmentionedintheActhavealsobeenlaiddowninaphasedmanner, defined as recentlyas April 2011. *Forthesakeofsimplicity,herewewillbeonlydiscussingthevariouspenaltyandoffencesdefinedasperprovisionsofITA2000andITAA2008.PleasenotethatwhereverthetermsITAct2000or2008areused,theyrefertosameactbecausetheITActnowincludesamendmentsasperIT2008Amendment Act.*
  Specificexclusion(s)totheActwhereitisnotapplicableare:
  - Negotiableinstrument(otherthanacheque)asdefinedinsection13ofthe Negotiable Instruments Act, 1881;
  - Apower-of-attorneyasdefinedinsection1AofthePowers-of-Attorney Act, 1882;
  - Atrustasdefinedinsection3oftheIndianTrustsAct,1882
  - Awillasdefinedinclause(h)ofsection2oftheIndianSuccessionAct,1925 including any other testamentary disposition

3. *Whatisacybercrime?*

Cyber Crime is not defined officially in IT Act or in any other legislation. In fact, it cannot be too. Offence or crimehasbeendealtwithelaboratelylistingvariousactsandthepunishmentsforeach,undertheIndianPenal Code, 1860 and related legislations. Hence, the concept of cyber crime is just a "combination of crime and computer".

Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets thesecurity of computer systems and the data processed by them.

Cybercrimeina broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

- Anycontractforthesaleorconveyanceofimmovablepropertyoranyinterestinsuchproperty;
- AnysuchclassofdocumentsortransactionsasmaybenotifiedbytheCentralGovernment

4. *CasesStudiesasperselectedITActSections*

HerearethecasestudiesforselectedITActsections.

ForthesakeofsimplicityandmaintainingclarIty,detailsontheITActsectionshavebeenomitted.KindlyreferttheAppendix at the last section for the detailed account of all the penalties and offences mentioned in IT Act.

- **Section 43 – Penalty and Compensation for damage to computer, computer system,etc*RelatedCase:MphasisBPOFraud:2005***InDecember 2004,fourcallcentreemployees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtainthePINs.Inassociationwithothers,thecallcentreemployeesopenednewaccounts at Indian banks using false identities.Within two months, they used the PINs and account information gleaned during their employment at MphasiS totransfer moneyfrom thebank accountsofCitiGroupcustomerstothenewaccountsatIndianbanks. By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recoveredwas $230,000.***Verdict***: *Court held that Section 43(a)was applicable here due to the nature of unauthorizedaccess involved to commit transactions.*
- **Section65–TamperingwithComputerSourceDocuments*RelatedCase:SyedAsifuddinandOrs. Vs. The State of Andhra Pradesh***In this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bitnumber(ESN) programmed intocell phones theft were exclusively franchised to Reliance Infocomm. ***Verdict:****Court held that tampering withsource code invokes Section 65 of the InformationTechnologyAct.*
- **Section 66 – Computer Related offenses*RelatedCase:Kumarv/sWhiteley***Inthiscasetheaccusedgainedunauthorizedaccessto theJointAcademicNetwork(JANET)anddeleted,addedfilesandchangedthepasswords todenyaccesstotheauthorizedusers.InvestigationshadrevealedthatKumarwasloggingonto the BSNL broadband Internet connectionasif he wasthe authorized genuine user and 'madealterationinthecomputerdatabasepertainingtobroadbandInternetuser accounts'ofthesubscribers.TheCBIhadregisteredacybercrimecaseagainstKumarandcarriedoutinvestigationsonthe basisofa complaintby the PressInformation Bureau, Chennai, which detected the unauthorised use of broadband Internet. Thecomplaint also stated that thesubscribers had incurred a loss of Rs 38,248 dueto Kumar's wrongful act. Heusedto'hack'sitesfromBangalore,Chennaiandothercitiestoo,theysaid. ***Verdict:****The AdditionalChiefMetropolitanMagistrate,Egmore,Chennai,sentencedNGArunKumar,thetechiefromBangaloretoundergoarigorousimprisonmentforoneyearwithafineofRs5,000undersection420IPC (cheating)andSection66ofITAct(ComputerrelatedOffense).*
- **Section 66A – Punishment for sending offensive messages throughcommunicationservice**
  - ***Relevant Case #1: Fake profile of President posted by imposter***On September9,2010,theimpostermadeafakeprofileinthenameoftheHon'ble President Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regardingthefourfakeprofilescreatedinthenameofHon'blePresident on social networking website, Facebook.The said complaint stated that presidenthousehasnothingtodowiththefacebookandthefakeprofile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.
  - ***RelevantCase#2:BombHoaxmail***In2009,a15-year-oldBangalore teenagerwasarrestedbythecybercrimeinvestigationcell(CCIC)ofthecity crimebranchforallegedlysendingahoaxe-mailtoaprivatenews channel.Inthee-mail,heclaimedtohaveplantedfivebombsinMumbai, challengingthepolicetofindthembeforeitwastoolate.Ataround1p.m. on May25,thenewschannelreceivedane-mailthatread:"Ihave plantedfivebombsinMumbai;youhavetwohourstofindit."Thepolice, who werealertedimmediately,tracedtheInternetProtocol(IP)address toVijayNagarinBangalore.TheInternetserviceproviderfortheaccountwas BSNL, said officials.
- **Section 66C – Punishment for identity theft *RelevantCases:***
  - TheCEOofanidentitytheftprotectioncompany,Lifelock,ToddDavis's social security number was exposed by Matt Lauer on NBC's Today Show. Davis' identity was used to obtain a $500 cash advance loan.
  - Li Ming,agraduatestudent atWestChesterUniversityofPennsylvania faked his own death,complete with aforged obituaryin his local paper. Ninemonthslater,Liattemptedtoobtain anewdriver'slicensewiththe intention of applying for new credit cards eventually.
- **Section 66D – Punishment for cheating by impersonation by using computerresource*Relevant Case: Sandeep Vaghesev/s Stateof Kerala***Acomplaint filedbythe representative of aCompany, whichwas engaged inthe business of tradinganddistributionof petrochemicals inIndiaandoverseas,acrime was registered against nine persons, alleging offenses under Sections 65, 66, 66A,C andD of the InformationTechnologyAct along withSections 419 and420of theIndianPenalCode.Thecompanyhasaweb-siteinthenameandandstyle

`www.jaypolychem.com’ but, anotherwebsite`www.jayplychem.org’wassetupintheinternetbyfirstaccusedSamdeep

Varghese@Sam,(whowasdismissedfromthecompany)inconspiracywithother accused,includingPreetiandCharanjeetSingh,whoarethesisterandbrother-in-lawof `Sam'
Defamatoryandmaliciousmattersaboutthecompanyandits directors weremadeavailable in that website. The accusedsister and brother-in-law were based in Cochin and they had been acting in collusion known and unknown persons, who have collectively cheated the companyandcommittedactsofforgery,impersonationetc. Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. tomalignthe name and image of the Companyand its Directors. The defamation campaign run by allthe said persons named above has caused immense damagetothenameandreputationoftheCompany. The Company suffered losses of several crores of Rupees from producers, suppliers and customers and were unable to do business.

- **Section 66E – Punishment for violation of privacy** ***RelevantCases:***
  - ***Jawaharlal Nehru University MMS scandal***In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university.Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones,ontheinternetandevensolditas aCDinthebluefilmmarket.
  - ***Nagpur Congress leader's son MMS scandal***On January 05, 2012 Nagpur Police arrested two engineering students, one of them ason of aCongressleader,forharassinga16-year-oldgirlbycirculatinganMMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, azilaparishad member and aninfluentialCongressleader of Saoner region in Nagpur district.
- **Section-66F Cyber Terrorism*****Relevant Case:***The Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspecthas been detained inthis case.Thepolicesaid an emailchallenging thesecurity agencies to prevent a terror attack was sent by one Shahab Md with an IDsh.itaiyeb125@yahoo.in to BSE's administrative email IDcorp.relations@bseindia.com at around 10.44 am on Monday.TheIP address of thesender has been traced to Patna in Bihar. TheISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, whilecreating the new ID, given two mobile numbers in thepersonal details column. Both the numbers belong to a photoframe-maker in Patna,'' said an officer. ***Status:*** *The MRA Marg police haveregistered forgery for purpose of cheating, criminalintimidation cases under the IPC and acyber-terrorism case under the IT Act.*
- **Section 67 – Punishment for publishing or transmitting obscene material inelectronicform**
  RelevantCase:Thiscaseisaboutpostingobscene,defamatoryandannoyingmessage aboutadivorceewomanintheYahoomessagegroup.E-mailswereforwardedtothevictim for informationbytheaccusedthrough afalsee-mail account openedbyhiminthenameof the victim.Thesepostingsresultedinannoyingphonecallstothelady.Basedonthe lady'scomplaint,thepolicenabbedtheaccused.Investigationrevealedthathewasaknownfamily friend of the victim and was interested inmarrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again.Onherreluctancetomarryhimhestartedharassingherthroughinternet.
  Verdict:*The accusedwasfoundguiltyofoffencesundersection469,509IPCand67ofITAct2000.Heisconvicted and sentenced for the offence as follows:*
  - *Asper469ofIPChehastoundergorigorousimprisonmentfor2yearsandtopayfine of Rs.500/-*
  - *Asper509ofIPCheis toundergotoundergo1yearSimpleimprisonmentand to pay Rs 500/-*
  - *AsperSection67ofITAct2000,hehastoundergofor2yearsandtopayfineofRs.4000/-*

  All sentences were to run concurrently.The accused paid fine amount and he was lodged at Central Prison,Chennai. This is consideredthe first case convicted under section 67 of Information TechnologyAct 2000 in India.

- **Section67B–Punishmentforpublishingortransmittingofmaterialdepictingchildreninsexually explicit act, etc. in electronicform*****RelevantCase:****JanhitManch&Ors.v.TheUnionofIndia10.03.2010PublicInterestLitigation:*The petition sought a blanket ban on pornographic websites. The NGO had arguedthatwebsitesdisplayingsexuallyexplicitcontenthadanadverseinfluence,leading youth on a delinquent path.
- **Section 69– Powers to issue directions for interception ormonitoring or decryptionofany information through any computer**

resource*Relevant Case:*In August 2007, Lakshmana Kailash K., a techiefrom Bangalore was arrestedonthesuspicionofhavingpostedinsultingimages ofChhatrapatiShivaji,amajor historicalfigure in thestate of Maharashtra, onthe social-networkingsite Orkut.The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's

ISP.HewasbroughttoPuneanddetainedfor50daysbeforeitwasdiscoveredthattheIP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m. ***Verdict:****Taking cognizance of his plight from newspaper accounts, the State HumanRightsCommissionsubsequentlyordered the company to payRs 2 lakh toLakshmanaasdamages.Theincident highlights how minor privacy violations by ISPs and intermediariescould have impactsthat gravely undermine other basic human rights.*

5. *CommonCyber-crimescenariosandApplicabilityofLegalSections*

Letuslookintosomecommoncyber-crimescenarios whichcanattractprosecution asperthepenaltiesand offences prescribed in IT Act 2000 (amended via 2008) Act.

- **Harassmentviafakepublicprofileonsocialnetworkingsite**A fake profile of a person is created on a social networking site with the correct address, residentialinformationorcontactdetailsbuthe/sheis labelledas‘prostitute’orapersonof ‘loosecharacter’.Thisleadstoharassmentofthevictim.*ProvisionsApplicable:-Sections66A,67 ofIT Act and Section 509 of the Indian Penal Code.*
- **Online Hate Community**Onlinehatecommunityiscreated inciting a religious group to act or pass objectionable remarksagainstacountry,nationalfiguresetc.*ProvisionsApplicable:Section66AofITActand153A& 153B of the Indian Penal Code.*
- **Email Account Hacking**If victim’s email account is hacked and obscene emails aresent topeople in victim’s address book.*Provisions Applicable:- Sections43, 66, 66A, 66C, 67, 67A and 67B of IT Act.*
- **Credit Card Fraud**Unsuspectingvictimswoulduseinfectedcomputerstomakeonlinetransactions.*ProvisionsApplicable:-Sections43,66,66C,66DofITActand section 420 of the IPC.*
- **Web Defacement** Thehomepageofawebsiteisreplacedwithapornographicordefamatorypage. Government sites generally face the wrath of hackers on symbolic days.*ProvisionsApplicable:- Sections43and66ofITActandSections66F,67and70ofITActalsoapplyinsomecases.*
- **IntroducingViruses,Worms,Backdoors,Rootkits,Trojans,Bugs**Allofthe above are some sort of malicious programs which are used to destroy or gain accesstosomeelectronicinformation.*ProvisionsApplicable:-Sections43,66,66AofITActandSection 426 of Indian Penal Code.*
- **Cyber Terrorism** Manyterrorists areusevirtual(GDrive,FTPsites)andphysicalstoragemedia(USB’s,hard drives) for hiding information and records of their illicit business.*ProvisionsApplicable:Conventional terrorism laws may apply along with Section 69 of IT Act.*
- **Online sale of illegal Articles**Where sale of narcotics, drugs weapons and wildlife is facilitated bythe Internet*ProvisionsApplicable:- Generally conventional laws apply in thesecases.*
- **Cyber Pornography** Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is.*Provisions Applicable:- Sections 67, 67A and 67B of theITAct.*
- **Phishing and EmailScams**Phishinginvolvesfraudulentlyacquiringsensitiveinformationthroughmasqueradingasiteasatrustedentity.(E.g.Passwords,creditcard information)*Provisions Applicable:- Section66, 66A and 66D of IT Act and Section 420 of IPC*
- **Theft of ConfidentialInformation**Manybusinessorganizationsstoretheirconfidentialinformationincomputersystems.This informationistargetedbyrivals,criminalsanddisgruntledemployees.*ProvisionsApplicable:- Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.*
- **Source Code Theft**A Source code generally is the most coveted andimportant“crownjewel” asset of acompany.*Provisionsapplicable:- Sections43,66, 66B of IT Act and Section 63 of Copyright Act.*
- **Tax Evasion and MoneyLaundering**Moneylaunderersandpeopledoingillegalbusinessactivitieshidetheirinformationinvirtual as well as physicalactivities.*ProvisionsApplicable: IncomeTax Actand Prevention of MoneyLaundering Act. IT Act may apply case-wise.*
- **Online Share TradingFraud**Ithasbecomemandatoryforinvestorstohavetheirdemataccountslinkedwiththeironline banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.*Provisions Applicable: Sections 43, 66, 66C, 66D of ITAct and Section 420 of IPC*

6. *Appendix*

I. **Penalties,CompensationandAdjudicationsections**

- **Section43–PenaltyandCompensationfordamagetocomputer, computer system**If any personwithout permissionof the owner or any other person who is in-charge of a computer, computer system or computer network –

- Accessesorsecuresaccessto suchcomputer,computersystem or computer network or computer resource

- Downloads,copiesorextractsany data,computerdata,computer databaseorinformationfromsuch computer,computersystemor computernetworkincluding information or data held or stored inanyremovablestoragemedium;
- Introducesorcausestobeintroduced any computer contaminantorcomputervirusinto anycomputer,computersystemor computernetwork-
- Damages orcausestobe damagedanycomputer,computer systemorcomputernetwork,data, computerdatabase,oranyother programmes residing in such computer, computer system or computernetwork-
- Disrupts or causes disruption of any computer, computer system, or computer network;
- Deniesorcausesthedenialof accesstoanypersonauthorisedto accessanycomputer,computer systemorcomputernetworkby any means
- Chargestheservicesavailedofby apersontotheaccountofanother personbytamperingwithor manipulatinganycomputerofa computer,computersystemor computernetwork-
- Providesanyassistancetoany persontofacilitateaccesstoa computer,computersystemor computernetworkincontravention oftheprovisionsofthisAct,rules orregulationsmadethere under,
- Chargestheservicesavailedofby apersontotheaccountofanother personbytamperingwithor manipulating any computer, computersystem,orcomputer network,
- Destroys,deletesoraltersany informationresidinginacomputer resourceordiminishesitsvalueor utilityoraffectsitinjuriouslybyany means,
- Steals,conceals,destroysor altersorcausesanypersonto steal,conceal,destroyoralterany computer source code used for a computerresourcewithan intentiontocausedamage,

heshallbeliabletopaydamagesbywayof compensation to the person so affected.

- **Section43A–Compensationforfailuretoprotectdata**Whereabodyc orporate,possessing,deali ngor handlinganysensitivepersonaldataorinformationina computerresourcewhichitowns,controlsor operates,isnegligentinimplementingandmaintainingre asonablesecuritypracticesand proceduresandtherebycauseswrongfullossor wrongfulgaintoanyperson,suchbodycorporate shallbeliabletopaydamagesbywayofcompensation,not exceedingfivecrorerupees,tothe person so affected.
- **Section 44 – Penalty for failure tofurnishinformationorreturn,etc.**Ifanype rsonwhois

requiredunderthisActoranyrulesorregulations made there under to –

- Furnishanydocument,returnor reporttotheControllerorthe CertifyingAuthority,failstofurnishthe same,he shallbeliable toa penaltynotexceedingonelakh andfiftythousandrupeesforeach suchfailure;
- File any return or furnish any information, books or other documents within the time specifiedthereforeinthe regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:
- Maintainbooksofaccountor records,fails tomaintainthesame, he shall be liable to a penalty not exceedingtenthousandrupeesfor everydayduringwhichthefailure continues.

- **Section 45 – Residuary Penalty**Whoever contravenesanyrulesorregulationsmadeunderthisAct,forthecontraventionofwhichnopenaltyhas beenseparatelyprovided,shallbeliabletopaya compensationnotexceedingtwenty-fivethousand rupees to the person affected by such contravention orapenaltynotexceedingtwenty-fivethousand rupees.
- **Section47–Factorstobetakenintoaccountbytheadjudicatingofficer**Section47lays downthat whileadjudgingthe quantumofcompensationunderthisAct,an adjudicatingofficershallhavedueregardtothe following factors, namely :-
    - Theamountof gainofunfair advantage, wherever quantifiable, made as a resultofthe default;
    - Theamountof losscausedto thepersonasa resultofthe default,
    - The repetitive nature of the default.

II. **Offencessections**

- **Section 65 – Tampering with ComputerSourceDocuments**Ifanypersonknowinglyorintentionallyconceals,destroyscodeoraltersor causes anothertoconceal, destroycode or alter any computer,computerprogram,computersystem,or computer network,heshallbepunishablewithimprisonmentupto threeyears,orwithfineuptotwolakhrupees,or with both.
- **Section–66ComputerRelatedOffences**Ifany person,dishonestly,orfraudulently,doesanyact referred to in section 43,he shall be punishable with imprisonmentforatermwhichmayextendtotwo threeyearsorwithfinewhichmayextendtofivelakhrupees or with both.
- **Section 66A – Punishment for sendingoffensivemessages through communicationservice**Any personwhosends,bymeansofacomputerresourceora communication device,
    - Any information that is grossly offensive or has menacing character;

- Anyinformationwhichheknowstobefalse,butforthepurposeof causing annoyance, inconvenience, danger, obstruction,insult,injury, criminal intimidation,enmity,hatred,orill will,persistentlymakesbymaking use ofsuchcomputerresourceor a communication device,
- Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to misleadtheaddresseeorrecipient abouttheoriginofsuchmessages

shallbepunishablewithimprisonmentforaterm which may extend to three years and with fine.

- **Section66B–Punishmentfordishonestlyreceivingstolencomputer resource orcommunicationdevice.**Whoever dishonestly receivesor retains any stolen computer resource or communication device knowingorhaving reason to believe the same to be stolen computer resource or communication device,shall be punished withimprisonmentofeitherdescriptionforaterm which may extend to three yearsor with fine which may extend to rupees one lakh or with both.
- **Section66C–Punishmentforidentitytheft**Whoever, fraudulentlyordishonestlymakeuseoftheelectronicsignature,passwordoranyotheruniqueidentificationfeature ofanyotherperson,shallbe punishedwithimprisonmentofeitherdescription foraterm whichmayextendtothreeyears andshall alsobeliabletofinewhichmayextendtorupeesone lakh.
- **Section 66D – Punishment for cheatingbypersonation by using computerresource**Whoever, by means of any communicationdevice or computer resource cheats bypersonating; shall be punished with imprisonment of either description for a term which may extend to threeyears andshall alsobeliabletofinewhichmay extend to one lakh rupees.
- **Section66E–Punishmentforviolationofprivacy**Whoever,intentionallyorknowinglycaptures, publishes or transmits the image of a privateareaofanypersonwithouthisorherconsent,under circumstancesviolatingtheprivacyofthat person,Explanation–Forthepurposesofthis section:
  - “transmit” means to electronically sendavisual image with the intent that it be viewed by a person or persons;
  - “capture”, with respect to an image,means to videotape, photograph,film orrecordby any means;
  - “privatearea” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
  - “publishes” means

the printed or electronic form and making it available for public;

- ○ “under circumstances violating privacy”means circumstances in which a person can have a reasonable expectation that–

  i. he or she could disrobe in privacy, without being concerned that an image of hi s private area was being captured; or

ii. any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

shallbepunishedwithimprisonmentwhichmayextendtothreeyearsor with fine not exceeding two lakh rupees, or with both.

7. **Section-66FCyberTerrorism**

I. Whoever,-

- with intent to threaten the unity, integrity, security or sovereigntyofIndiaortostriketerrorinthepeopleor any section of the people by –
  - denyingorcausethedenialof accesstoanypersonauthorizedto access computer resource; or
  - attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

- ○ introducingorcausingtointroduce anyComputerContaminantand bymeansofsuchconductcauses orislikelytocausedeathor injuriestopersonsordamagetoor destruction of property or disrupts orknowingthatitislikelytocause damageordisruptionofsupplies or servicesessential to the life of thecommunityor adverselyaffect the critical information infrastructure specified under section 70, or

- ▪ knowinglyorintentionallypenetratesoraccessesa computer resource without authorization or exceedingauthorizedaccess,andbymeansofsuch conductobtainsaccesstoinformation,dataorcomputerdatabasethatisrestrictedforreasonsofthe securityoftheStateorforeignrelations;orany restrictedinformation,dataorcomputerdatabase, withreasonstobelievethatsuchinformation,dataor computerdatabasesoobtainedmaybeusedto cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State,friendlyrelationswithforeignStates,public order, decencyor morality, or in relation tocontempt ofcourt,defamationorincitementtoanoffence,ortothe advantageofanyforeignnation,groupofindividualsorotherwise,commitstheoffenceofcyber terrorism.

II. Whoevercommitsorconspirestocommitcyberterrorismshallbe punishablewithimprisonmentwhichmayextendtoimprisonmentforlife.

8. **Section67–Punishmentforpublishingortransmittingobscenematerialinelectronicform**Whoeverpublishesortransmits orcausestobepublishedintheelectronicform,any materialwhichislasciviousorappealsto the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances,toread,seeorhearthemattercontainedorembodiedinit,shallbepunished on firstconviction with imprisonment of either description for aterm whichmay extend totwo threeyearsandwithfinewhichmayextendtofivelakhrupeesandintheeventofa second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

9. **Section67A–Punishmentforpublishingortransmittingofmaterialcontainingsexuallyexplicitact,etc.in electronic form**Whoever publishes or transmits or causes to be publishedortransmittedintheelectronicformanymaterialwhichcontainssexuallyexplicitactor conductshallbepunishedonfirstconvictionwithimprisonmentofeitherdescription foratermwhichmayextendtofiveyearsandwithfinewhichmayextendtotenlakhrupees andintheeventofsecondorsubsequentconvictionwithimprisonmentofeitherdescription foratermwhichmayextendtosevenyearsandalsowithfinewhichmayextendtotenlakh rupees.

10. **Section67B.Punishmentforpublishingortransmittingofmaterialdepictingchildrenin sexually explicit act, etc. in electronic form** Whoever:-

I. publishesortransmitsorcausestobepublishedortransmittedmaterial inanyelectronicformwhichdepictschildrenengagedinsexuallyexplicitact or conduct or

II. createstextordigitalimages,collects,seeks,browses,downloads, advertises,promotes,exchangesordistributesmaterialinanyelectronicformdepictingchildreninobsceneorindecentorsexuallyexplicit manner or

III. cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

IV. facilitatesabusingchildrenonlineor

V. records inany electronic form own abuse orthat of others pertaining to sexually explicit act with children,

shallbepunishedonfirstconvictionwithimprisonmentofeitherdescriptionforatermwhich mayextendtofiveyearsandwithafinewhichmayextendtotenlakhrupees andintheeventofsecondorsubsequentconvictionwithimprisonmentofeitherdescription foratermwhichmayextendtosevenyearsandalsowithfinewhichmayextendtotenlakh rupees: Providedthattheprovisions ofsection67,section67Aandthissectiondoes notextendto anybook,pamphlet,paper,writing,drawing,painting,representationorfigureinelectronic form

11. **Section69–Powerstoissuedirectionsforinterceptionormonitoringordecryptionofany information through any computer resource.-**

I. Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government,asthecasemaybe,inthisbehalfmay,ifissatisfiedthatit is necessary or expedient to do in the interest of the sovereignty or integrityofIndia,defenceofIndia,securityoftheState,friendlyrelations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

II. The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

III. Thesubscriberorintermediaryoranypersoninchargeofthecomputer resourceshall,whencalleduponbyanyagencywhichhasbeendirectedunder subsection(1), extend all facilities andtechnical assistanceto –

- provide access to or secure access to the computer resourcegenerating,transmitting,receivingorstoring such information; or
- interceptormonitorordecrypttheinformation,asthe case may be; or
- provideinformationstoredincomputerresource.

IV. The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonmentforatermwhichmayextendtosevenyearsandshallalso be liable to fine.

12. **Section69A–Powertoissuedirectionsforblockingforpublicaccessofanyinformationthrough any computerresource**

I. Wherethe Central Governmentoranyofitsofficerspeciallyauthorized byitinthisbehalfissatisfiedthatitisnecessaryorexpedientsotodoin theinterestofsovereigntyandintegrityofIndia,defenseofIndia,security of theState,friendlyrelationswithforeignstatesorpublicorderorfor preventingincitementtothecommissionofanycognizableoffence relatingtoabove,itmaysubjecttotheprovisionsofsub-sections(2)for reasonstoberecordedinwriting,byorderdirectanyagencyofthe Governmentorintermediarytoblockaccessbythepublicorcausetobeblocked foraccessbypublicanyinformationgenerated,transmitted, received, stored or hosted in any computer resource.

II. Theprocedureandsafeguardssubjecttowhichsuchblockingforaccessby the public may becarried out shall besuch as may be prescribed.

III. Theintermediarywhofailstocomplywiththedirectionissuedundersub-section(1)shallbepunishedwithanimprisonmentforatermwhichmay extend to seven years and also be liable to fine.

13. **Section69B.Powertoauthorizetomonitorandcollecttrafficdataorinformationthrough any computer resource for Cyber Security**

I. TheCentralGovernmentmay,toenhanceCyberSecurityandfor identification,analysisandpreventionofanyintrusionorspreadof computercontaminantinthecountry,bynotificationintheofficial Gazette,authorizeanyagencyoftheGovernmenttomonitorandcollecttraffic data or information generated, transmitted, received or stored in any computer resource.

II. TheIntermediaryoranypersonin-chargeoftheComputerresourceshallwhencalleduponbytheagencywhichhasbeenauthorizedundersub- section(1), providetechnical assistanceandextendallfacilitiestosuch agencytoenableonlineaccess ortosecureandprovideonlineaccess to thecomputerresourcegenerating,transmitting,receivingorstoring such traffic data or information.

III. Theprocedureandsafeguardsformonitoring andcollectingtrafficdataor information, shall be such as may be prescribed.

IV. Any intermediary who intentionally or knowingly contravenes the provisions of subsection(2)shallbe punishedwith animprisonment for a term which may extend to three years and shall also be liable to fine.

14. **Section71 –Penalty for misrepresentation**Whoever makes anymisrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic SignatureCertificate, as the casemay be,shall be punished with imprisonment for a term which may extend to two years, or withfine which may extend to one lakh rupees, or with both.

15. **Section72–Breach ofconfidentialityand privacy** Any person who, in pursuant of any ofthe powers conferred under this Act, rules or regulations made there under, has secured accesstoanyelectronic record, book, register,correspondence,information, document or other material without the consent of the person concerned discloses such electronic record,book,register,correspondence,information,documentorothermaterialtoany

otherpersonshallbepunishedwithimprisonmentforatermwhichmayextendtotwoyears,orwith fine which may extend to one lakh rupees, or with both.

16. **Section72A–PunishmentforDisclosureofinformationinbreachoflawfulcontract**Anyperson including an intermediary who, while providing services under the terms of lawful contract,hassecuredaccesstoanymaterialcontainingpersonalinformationaboutanotherperson, withtheintenttocauseorknowingthatheislikelytocausewrongfullossor wrongful gain discloses, without the consent of the person concerned, or in breach ofa lawful contract, suchmaterial to any other person shall be punishedwith imprisonment for atermwhichmayextendtothreeyears,orwithafinewhichmayextendtofivelakhrupees,orwith both.

17. **73.PenaltyforpublishingelectronicSignatureCertificatefalseincertainparticulars.**

    I. No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

        - theCertifyingAuthoritylistedinthecertificatehasnot issued it; or
        - thesubscriberlistedinthecertificatehasnot accepted it; or
        - thecertificatehasbeenrevokedorsuspended, unlesssuchpublicationisforthepurposeofverifying adigitalsignaturecreatedpriortosuchsuspensionor revocation

    II. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for aterm which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

18. **Section 74 – Publication for fraudulent purpose:**Whoever knowingly creates, publishesor otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purposeshall bepunishedwithimprisonmentforatermwhichmayextendtotwo years, or with fine which may extend to one lakh rupees, or with both.

19. **Section75–ActtoapplyforoffenceorcontraventionscommittedoutsideIndia**

    I. Subject to the provisions of sub-section (2), the provisions of this Act shallapplyalsotoanyoffenceorcontraventioncommittedoutsideIndia by any person irrespective of his nationality.

    II. Forthepurposes ofsub-section(1),thisActshallapplytoanoffenceor contraventioncommittedoutsideIndiabyanypersonif theact orconduct constitutingtheoffenceorcontraventioninvolvesacomputer,computer system or computer network located in India.

20. **Section77A–CompoundingofOffences.**

    I. A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceedingthreeyearshasbeenprovidedunderthisAct.Providedfurtherthat the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

    II. Thepersonaccusedofanoffenceunderthis actmayfileanapplication forcompoundinginthecourtinwhichoffenceispendingfortrialandthe provisions of section 265 B and 265C of Code of Criminal Procedures, 1973 shall apply.

21. **Section 77B – Offences with three years imprisonment to be cognizable**Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishablewithimprisonmentofthreeyearsandaboveshallbecognizableandtheoffence punishable with imprisonment of three years shall be bailable.

22. **Section 78 – Power to investigateoffences**NotwithstandinganythingcontainedintheCodeofCriminal Procedure,1973,apoliceofficernotbelowtherankofInspectorshallinvestigateany offence under this Act.

Liabilityoftheinternetserviceprovider:

TableofContents

Introduction

With the advent of the internet, there has become a parallel world in cyberspace where people connect, relate and communicate.Theworldof cyberspaceisdrivenby data, datathat is availabletopublish, useanddisposal of the internet. Data spans across all kinds of content from written, textual, audio, video and other media and entertainment-relatedcontenttobusiness-relatedcontent,alloftheseareaccessed,usedandconsumedbythe masses who put forward their trust and participate in this giant data exchange we call the cyber community. Needless to say, the trust comes on one end towards the genuine of data being projected and consumed, and more its authenticity is of utmost importance, on the other hand, the privacy of the people accessing the information, content and services offered is of utmost and crucial importance.

As the internet and digital consumption advanced through time, it becamemore and more crucial to bring in mechanismstocheckandcontroltheauthenticity,securityandprivacyofdata.Frompiracy tophishingtodata leaks, tamperingofinformation,misguidingandmisleadinginformation,fakeimpostersandallkindsof inauthenticcontentfromconspiracytheoriestoonlinescamsandscandal,impostersandfakeporn,theinternet werebecomingabanetomankindasmuchitwasabooninintegratingtheworldintoonebiggiantcommunity. But just like society, cyberspace also had its perils with authenticity and infringement of data being the determinant source of all problems.

WhatisanISP?

Let us look at cyberspace as the digital form of the world, wherein real-world road, air and rail networks were the access to travel, offered by the respective states and their governments, the networkaccess to people on cyberspaceto surfwasbroughtaboutby theISP’s,theinternetservicesproviders.Inthesimplestterms,tobe an intermediaryistobelikeaconduitforthepassageofanyinformation/communication.Theyactlike aggregatorsbetweenthosewhowantedtogenerateandspreadinformationandthosewhowantedtoconsume information.Needlesstosay,whenthetimecamewherethedubiousandinauthenticinformationhadbecomeanuisance forglobalpeace,economy,trade,etc.Therewasaneedtoregulateandcontroltheinformationon theinternet,andsinceitwasdifficulttokeeptrackofindividualsworldwide,itwasdonethroughthesourcethatactedasa medium to aggregate this connectivity, the ISP’s, the internet service providers.

The issue of online copyright infringement liability for the ISP’s thus became prevalent since the use of the internetstartedtoexpandrapidly.TheimperativequestionthatariseshereistowhatextentareISPsresponsible for the third party material put on the internet by users of their facilities?

Because of the hurdles and constraints on keeping track and catching hold of individuals on a worldwide level, because of geo-cultural, geopolitical and simply inability of copyright and intellectual property owners to seek infringement damages against those who misappropriate their intellectual or digital properties, the internet serviceprovidershavebecomeanaccessiblemuletoaddressthisproblem,namelysincethey allowtheinternet or data pirates to exist, for which reason the content owners find it righteous to sue the ISP’s for their data infringement because the ISP’s naturally are in a position to control and secure the internet through plausible policing.

In this paper, we explore the role of the ISP’s communication on the internet, their various approaches for determining the liability of the ISP’s for eg. the horizontal approach, the non-horizontal approach and explain the liability of ISPs for copyright infringement under theCopyright Act, 1957, and theInformationTechnologyAct, 2000.

ISP’sroleincommunicationontheinternet

ISPisthegatewayoranaggregatorthatprovidesthenetworkinfrastructure,incommonparlance,abandwidth (road network)whichgivespeopleaccesstonavigatethroughtheworldwidewebandaccessdataand informationononeend,andontheother,theygivehostingandwebsitebuildingandothersuchservicesforthesupplyof dataandcontent.OtherthanISP’svariouspartiesareinvolvedinofferingsolutionsforcreating, storing,hosting,deliveringandaccessinginformationandcontentfromthecontentcreatortothecontent consumerssuchasbloggingsites,cloudplatforms,hostingservers,databaseservers,etc.attheendoftheday all the informationgetsstoredinaserverandisaccessedfromthatserversthroughtheinternet.Incommon parlance, theserver is an address whereoneseeks to access theinformation through thehighwayand road networkwhichisprovidedbytheISPthroughtheinternetandbandwidth,tobeabletonavigateandaccessthe informationstoredontheseservers.Thevariousintermediariesthathost,store,processdataanddataservicesareall connected to the content providers onone end and the consumerson theother through theISP’s which are the roadnetworkthatenablesthetransportofinformationandpeople(albeitvirtually)betweenonepointto another.

The website host deploys servers where FTP's, file transfer protocols are deployed for storing, accessing andtransporting files, website hosting is done on these servers. Thesedays cloudcomputing offers remote storage ofdatathatcanbeaccessedonmultiplepoints.Uponstorage,onsuchserversandcloudservers,thisdatagets availedtoanybodywithaninternetconnectionandtheaddresstotheserverlocation.Anaccessproviderontheotherhand provides access to the internet. In the process, all this is happening through the network infrastructure of the internet service provider, ISP. This network infrastructure transports this data to the designatedconsumer.ISP'sareaggregatorswhocreateaccessandnetworktotransportinformationexchange.

Liabilityofinternetserviceprovider

The liability for copyright infringement rests on three theories; direct, vicarious and contributory infringement. Direct infringement occurs when a person violates any exclusive right of the copyright owner. Vicarious liability ariseswhenapersonfailstopreventinfringementwhenhecanandhasarighttodosoandisdirectlybenefited by such infringement.

IntheUnitedStates,oneoftheActswhichprovidesliabilityfortheISPsistheDigitalMillenniumCopyrightAct, 1998. This Act governs the liability of the internet sites and ISPs for the copyright infringement of its user. It provides a mechanism for copyright owners to force site owners and ISPs to remove infringing material.

ThefollowingelementsarepartoftheregimeundertheDMCA:

1) Theonlineserviceprovider[hereinafterOSP]musthaveadesignatedagenttoreceivenoticesanditmust use a public portion of its Web site for receipt of notices;

2) TheOSPmustnotifytheU.S.CopyrightOfficeoftheagent'sidentityandtheCopyrightOfficewillalso maintain electronic and hard copy registries of Web site agents.

Variousapproachestodeterminetheliabilityofinternetserviceproviders

The scope of an ISP's liability extends to the branch of law pertaining and relating to the content and subject matterinquestion.Itcouldbeprivateorpersonal,criminal,tort,intellectualpropertylikecopyright,trademark, patent, etc., competition law, consumer protection, etc. and thus the liability of the ISP's has been burning, constantly evolving and expanding. These have been done broadly through two approaches:

1. Horizontalapproach

Which covers not just copyright infringement but all other areas and branches of law, where the liability of ISP arises directly and itraises fixed liabilities irrespective of the content and extentof the illegality of the content.

2. Non-horizontalapproach

The potential of the liability is determined by the provisions and jurisdictions of the law. In this approach, the statutesdeterminetheextentofliability,inwhichacaseofdefamationwouldbecoveredunderdefamationlaws, copyrightinfringementwouldbecoveredunderintellectualpropertyrightslaw,harmtoperson,deathandrape threats would be covered under IPC, etc.

Copyright is dealt with preserving the efforts and performance of the intellect. The concern of copyright is the protectionofliteraryandartisticworks.Theseconsistofmusic,writings,theeffortsofthefinearts,music,such assculpturesandpaintings,technology-basedworkssuchascomputerprogramsandelectronicdatabases.The liabilityforcopyrightinfringementrestsonthreetheories-direct,vicariousandcontributoryinfringement.Direct infringement occurs when a person violates any exclusive right of the copyright owner. Vicarious liability arises when a person fails to prevent infringement when he can and has a right to do so and is directly benefited by suchinfringement.Thesetwotheoriesarebasedonthestrictliabilityprincipleandapersonwillbeliablewithout any regardtohismentalstateorintention.Contributoryliabilityariseswhenapersonparticipatesintheactof directinfringementandhasknowledgeoftheinfringingactivity.Thequestionarisesastowhichstandardshould be applied in order to fix the responsibility of service providers.

LawSikho
Diploma in
Cyber Law, FinTech Regulations and Technology Contracts
Course Duration: 12 Months
in association with
Download free study material

ProvisionsundertheIndianCopyrightAct,1957

The Indian Copyright Act is unable to protect the unauthorized distribution and use of work over the internet. Infringementovertheinternetandpiracyposesathreattocreativeworksworldwideandthusthegrowthoftheinternet,e-commerceand thedigitaleconomy.Thelaw related toISPliability is vague and ambiguous inIndia. The Indian Copyright Act 1957, though amended in 1994 and 1197, doesn't cover or even mention copyrightinfringements and liability of ISPs regarding them.

The crux of copyright infringement according to the Act is that whether a person is gaining economic gains out of theinfringementandincaseofISPsliability, theISPsaregaining any directeconomicgainsoutof copyright infringement.UsershoweverdopayISPsforusinginternetservices,buttheyusuallygetawaywiththeexcuse thattheydidnotknowtheiractswereintheviolenceofownerscopyrights.Moreover,Section63ofthecopyright Act,1957providesforabutmentregardstocopyrightinfringements,butwhetherISPscanbesaidtobeabetting wouldagainbeacasetobsettledinthecourtoflawsinceISPsclearlywouldstatenointentionastheirbasisto avoid legal liability.

TheseissueshavebeenaddressedinSection79oftheInformationTechnologyAct,2000.

ProvisionsunderInformationTechnologyAct,2000

Chapter XIIof the Act provides for issues regarding the liability of the service providers. The Act refers to ISPs as 'network service providers' and exempts them from their liability.Section 79 absolves the ISP's liability if they can prove theyhad noknowledge about the infringement or due diligence was exercised for prevention of such acts. The Indian position in liability of service providers for copyright infringement must be made more explicit. The Act must include sections that address the financial aspect of the transaction, and the relationship betweenanISPand athird party,because this isvital todetermining the identity of theviolator.The American concept of contributory infringement can also be incorporated into the Indian Act so that if any person with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, the person can be made liable.

In order to be exempt from liability, the Indian Act requires the service provider to exercise due diligence to prevent the commission of copyright infringement. The Act does not provide the meaning of the term due diligence. If due diligence means policing each and every aspect of the internet,it can lead to loss of privacyand can ultimately have a disastrous effect. There is a need for a consensus on the meaning of the term due diligencebecausetheprimaryfunctionofISPsistobuildtheinternet,nottoplaytheroleofapoliceman.Ifthe behaviour of an ISP is reasonable, then that ISP should not be held liable for each and every activity on the internet as has been held by the US courts.

Variousinternationalscenarios

The WIPO Copyright Treaty, 1996 first caught international attention on copyrights. The treaties updated the BerneConventionbyincorporatingtheexistingTRIPSprovisionsinitsfoldsandgrantedadditionalrightstothe authors in the context of the internet. A new right referred to as the right of communication to the public wasincorporated and the right of distribution was specifically spelt out. It also provided for legal remedies against thecircumventionoftechnologicalmeasuresusedbytheauthorstoprotecttheirwork.Legalprotectionwasalso granted to rights management information systems used by the authors while transmitting works in a digital environment. It was further made clear that mere provision of physical facilities for enabling or making a communication does not itself amount to communication with the meaning of this provision.

Since there was no agreement to treat both temporary and permanent reproduction as a part of reproduction rights indigital format, nospecific provisionwas includedintheWCT inthis regard.It was thefailureofthe internationalcommunityduetothepressurefrominterestgroupstoreachadefinitiveconclusiononthenature of the liability of service providers and users, that left the international law unsettled and it was left to the respective NationStatestointroduceappropriateprovisionsinthedomesticlawtoprotecttheinterestsofthe owners.OneofthefirstcountriestolegislateontheTreatyprovisionswastheUSthroughitsDigitalMillennium Copyright Act (DMCA) that came into force in1998. Before referring to the DMCA it is necessary to refer to some of thejudicialpronouncementsofUSCourtsontheissue.In*PlayboyEnterprisesv.Frena*,thecourtwas calledupontodeterminetheliabilityoftheelectronicBulletinBoardSystem(BBS)operatorfortheactsofuserswhohad uploadedanddownloadedtheplaintiff'scopyrightedphotographs.ThecourtfoundFrenaliablefor violatingtheplaintiffsrighttopubliclydistributeanddisplaycopiesofitswork.Thedefendantcontendedthathe hadinfactremovedthephotographsfromtheBBSwhenhereceivedthecomplaintandhadsincemonitoredthe BBS to prevent additional photographs of Playboy from being uploaded.

Internetserviceprovidersbeingmadeliabletosuitforcopyrightinfringementontheinternet

Frequentlyincopyrightinfringementssuitsbeingfiledforactionsofinfringementontheinternet mostcertainly involvetheISPs.ThereasonbeingthatISPsarefarmoreinasuperiorpositiontopolice,trackandtakeactionincasesof piracyorinfringement,thananownerwhowillberathercompletelyunawareofthewhereaboutsof suchinfringementstakingplace,theISPswouldhavetheinternettrafficdatarelatingtosuchactivitiesthatshowdownloads of the infringed product. But ISPs are large business bodies or corporations with deep pockets and withconcentratedmarketshare,soitisalmostdifficulttoseealikelyoutcomesinceoneinfringementwillresultincausing many more.

CyberAppellateTribunal

TheInformationTechnologyAct,2000alsoprovidesfortheestablishmentoftheCyberAppellateTribunal.Inthisarticle,wewilllookattheestablishment ,composition,jurisdiction,powers,andproceduresifaCyberAppellateTribunal.

Tableofcontent

SuggestedVideos

StudyofCyberCrimes

IntroductionofInformationTechnologyAct2000Part1

IntroductionofInformationTechnologyAct2000

EstablishmentofCyberAppellateTribunal(Section48)

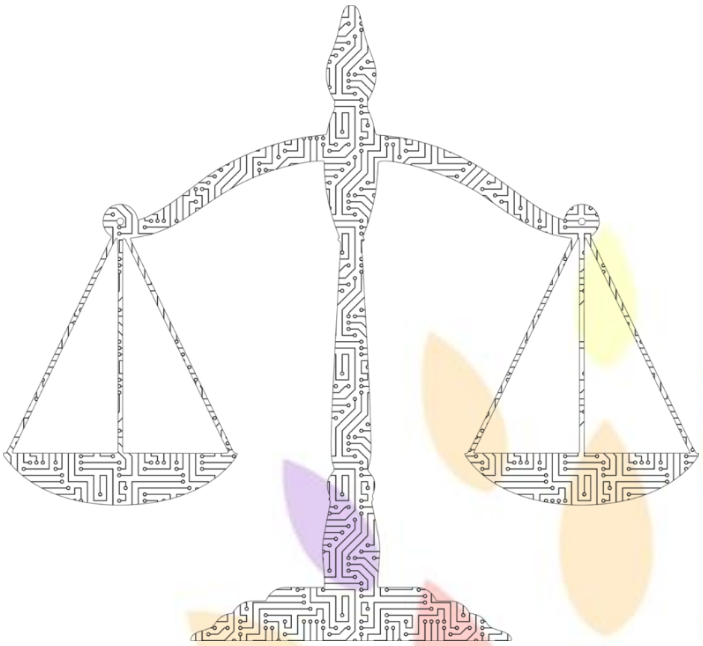
1. TheCentralGovernmentnotifiesandestablishesappellatetribunalscalledCyberRegulationsAppellateTribunal.
2. TheCentralGovernmentalsospecifiesinthenotificationallthemattersandplaceswhich fallunderthejurisdictionoftheTribunal.

BrowsemoreTopicsunderCyberLaws

- IntroductiontoCyberspace
- DigitalSignature
- RegulationofCertifyingAuthorities
- ClassificationandProvisionofCyberCrimes
- ScopeofCyberLaws
- ElectronicRecordandE-Governance
- InformationTechnologyAct,2000

ThecompositionofCyberAppellantTribunal(Section49)

TheCentralGovernmentappointsonlyonepersoninaTribunal–thePresidingOfficeroftheCyberAppellateTribunal.



Source:Pixabay

ThequalificationsforappointmentasPresidingOfficeroftheCyberAppellateTribunal(Section50)

ApersonisconsideredqualifiedfortheappointmentasthePresidingOfficerofaTribunalif–

a. HehasthequalificationoftheJudgeofaHighCourt

b. HeisorwasthememberoftheIndianLegalServiceandholdsorhasheldapostinGradeIofthatserviceforatleastthreeyears.

TheTermofOffice(Section51)

TheTermofOfficeofthePresidingOfficerofaCyberAppellateTribunalisfiveyearsfromthedateofenteringtheofficeoruntilheattainstheageof65years,whichever is earlier.

Fillingupofvacancies(Section53)

Ifforanyreasonotherthantemporaryabsence,thereisavacancyintheTribunal,thentheCentralGovernmenthiresanotherpersoninaccordancewiththeActtofillthevacancy. Further,theproceedingscontinuebeforetheTribunalfromthestageat whichthevacancyisfilled.

Resignationandremoval(Section54)

1. ThePresidingOfficercanresignfromhisofficeaftersubmittinganoticeinwritingtotheCentralGovernment,provided:

    a. heholdsofficeuntiltheexpiryofthreemonthsfromthedatetheCentralGovernmentreceivessuchnotice(unlessthe Government permits him to relinquish his office sooner), OR

    b. heholdsofficetilltheappointmentofasuccessor,OR

    c. untiltheexpiryofhisoffice;whicheverisearlier.

2. In caseofprovenmisbehaviourorincapacity,theCentralGovernmentcanpassanordertoremovethePresidingOfficeroftheCyberAppellate Tribunal. However, this is only after the Judge of the Supreme Court conducts an inquiry where thePresidingOfficerisawareofthe chargesagainsthimand hasa reasonableopportunitytodefend himself.

3. TheCentralGovernmentcanregulatetheprocedurefortheinvestigationofmisbehaviourorincapacityofthePresidingOfficer.

OrdersconstitutingAppellateTribunaltobefinalandnottoinvalidateitsproceedings(Section55)

Accordingtothissection,noorderoftheCentralGovernmentappointinganypersonasthePresidingOfficeroftheTribunalcanbequestionedinanymanner.Further,noonecanquestionanyproceedingbeforeaCyberAppellateTribunalinanymannermerelyonthegroundsofanydefectinthe Constitutionof theTribunal.

AppealtoCyberAppellateTribunal(Section57)

1. Subjecttotheprovisionsofsub-section(2),apersonnotsatisfiedwiththeControllerorAdjudicatingOfficer'sordercanappeal to the Cyber Appellate Tribunal having jurisdiction in the matter.

2. NoappealshalllietotheCyberAppellateTribunalfromanordermadebyanadjudicatingofficerwiththeconsentoftheparties.

3. Thepersonfilingtheappealmustdosowithin25daysfromthedateofreceiptoftheorderfromtheControllerorAdjudicatingOfficer.Further,hemustaccompanytheappealwiththeprescribedfees.However,iftheTribunalissatisfiedwiththereasonsbehindthedelay of filingtheappeal,then it may entertain it even after theexpiry of25 days.

4. Onreceivinganappealundersub-section (1),theTribunalgivesan opportunitytoallthepartiestotheappealtostatetheirpoints,before passing the order.

5. TheCyberAppellateTribunalsendsacopyofeveryordermadetoallthepartiestotheappealandtheconcernedControlleroradjudicatingofficer.

6. TheTribunaltriestoexpeditiouslydealwiththeappealsreceivedundersub-section(1).Italsotriestodisposeoftheappealfinallywithin six months of receiving it.

ProcedureandpowersoftheCyberAppellateTribunal(Section58)

1. TheCodeofCivilProcedure,1908doesnotbindtheCyberAppellateTribunal.However,theprinciplesofnaturaljusticeguideitanditissubjecttootherprovisionsoftheAct.TheTribunalhaspowerstoregulateitsownprocedure.

2. Inordertodischargeitsfunctionsefficiently,theTribunalhasthesamepowersasvestedinaCivilCourtundertheCodeofCivilProcedure, 1908, while trying a suit in the following matters:

   a. Summoningandenforcingtheattendanceofanypersonandexamininghimunderoath

   b. Ensuringtheavailabilityoftherequireddocumentsorelectronicrecords

   c. Receivingevidenceonaffidavits

   d. Issuingcommissionsforexaminingwitnessesordocuments

   e. Reviewingitsdecisions

   f. Dismissinganapplicationfordefaultordecidingitex-parte,etc.

3. EveryproceedingbeforetheCyberAppellateTribunalislikeajudicialproceedingwithinthemeaningofsections193and228andforthepurposesofsection196oftheIndianPenalCode.Further,theTribunalislikeaCivilCourtforthepurposesof section 195 andChapter XXVI of the Code of Criminal Procedure, 1973.

RighttoLegalRepresentation(Section59)

Theappellantcaneitherappearinpersonorauthorizeoneormorelegalpractitionerstopresenthiscasebeforethetribunal.

Limitation(Section60)

TheprovisionsoftheLimitationAct,1963,applytotheappealsmadetotheTribunal.

CivilCourtnottohavejurisdiction(Section61)

IftheITAct,2000empowerstheadjudicatingofficerortheCyberAppellateTribunalforcertainmatters,thennoCivilCourtcanentertainanysuitor proceedings for the same.

Further,nocourtcangrantaninjunctiononanyactionthatapersontakesinpursuanceofanypowerthattheActconfersuponhim.

AppealtoHighCourt(Section62)

Let'ssaythatapersonisnotsatisfiedwiththedecisionororderoftheTribunal.Insuchcases,hecanfileanappealwiththeHighCourt.Hemustdosowithin60daysofreceivingthecommunicationoftheorder/decisionfromtheTribunal.

Theappealcanbeonanyfactorlawarisingoutofsuchanorder.TheHighCourtcanextendtheperiodbyanother60daysifitfeelsthattheappellanthadsufficientcauseand reasonsforthedelay.

Compoundingofcontraventions(Section63)

1. TheControlleroranyotherofficerthatheortheadjudicatingauthorizesmaycompoundanycontravention.Compoundingispossibleeitherbeforeoraftertheinstitutionofadjudicationproceedings.Thisissubjecttotheconditionsthatthecontroller

orsuchotherofficerortheadjudicatingofficerspecifies.Provided,thesumdoesnotexceedthemaximumamountofpenaltythat theAct allows for the compounded contravention.

2. Nothinginsub-section(1)appliestoapersonwhocommitsthesameorsimilarcontraventionwithinaperiodofthreeyearsfromthedateonwhichhisfirstcontraventionwascompounded.Therefore,ifthepersoncommitsasecondcontraventionaftertheexpiryperiodofthreeyearsfromthedateonwhichhisfirstcontraventionwascompounded,thenthisbecomeshisfirstcontravention.

3. Onceacontraventioniscompoundedundersub-section(1),thennoproceedingispossibleagainstthepersonguiltyofthecompoundedcontravention.

RecoveryofPenalty(Section64)

Ifa penaltyimposedunderthisActisnotpaid,thenthesameisrecoveredasarrears oflandrevenue.Further,thelicenseordigitalsignaturecertificateissuspendeduntil the penalty is paid.

Penalties,CompensationandProcedureofAdjudicationunderITAct,2000

Introduction:

TheInformationTechnologyAct,2000wasimplementedon17May2000toprovidelegalrecognitionforelectronictransactionsandto promote e-commerce. It was subsequently amended with the passage of the Information Technology (Amendment) Act, 2008.

ThefollowingaretheimportantobjectivesofTheInformationTechnologyAct,2000:

1. Grantlegalrecognitionfore-transactions.
2. ProvidelegalrecognitionofDigitalAuthenticationSignatures.
3. Facilitatee-Dataandinformationfiling.
4. EnableElectronicdatastorage.
5. Grantacknowledgmentforthepreservationofbooksofaccountsinelectronicform.

Section43ofTheInformationTechnologyAct,2000

Penaltyandcompensationfordamagestodevice,computersystem(CS),orcomputernetwork(CNW)under Section43.[1]This sectionstatesthatifanindividualexecutes anyofthefollowingprohibitedactions,heshallbeliableforthedamagestotheparty concerned by paying compensation not exceeding 1 crore:

1. **Accesswithoutauthority:**Ifaccesstoorsecuresaccesstosuchadevice,computersystem,orcomputernetwork.
2. **Downloading,copying,orextractinganydatawithoutauthority:**Ifanydata,computerdatabase,orinformationis downloaded, copied, or extracted from any computer, computer system, or computer network.
3. **Injection of computer contaminant/virus:** If anycomputer contaminant or computer virus is imported or caused to beintroducedintoanycomputer,computersystem,orcomputernetwork,eveninformationordatastoredorstoredin any removable memory device.
4. **Damagestoacomputerdatabase:**Ifitdamagesorcausesdamagetoanycomputer,computersystem,orcomputer network,records,computerdatabase,orotherprogramswithinthatcomputer,computersystem,orcomputernetwork.
5. **Disjunctureofthecomputer,computersystem,orcomputernetwork:** Ifanydisruptionis causedtothespecified computerresources.
6. **Denial of access:**If it refuses or triggers denial of access by any means to any person authorized to access any device, computer system, or computer network.
7. **Providing aid to facilitate access:** If any support is given to any person to enable access to a device, computer system, or computer network in violation of theprovisions of this Act, therules or regulations thereunder shall apply.
8. **Charging services to another person's account:** If they charge a person's services to another person's account through tampering with or manipulating some CS or CNW device.
9. **Destruction,deletion,ormodificationofinformation:** Ifitdamages,deletes,orchangesanyinformationthatexists in a computer resourceor devalues its value or usefulness or affects it injuriouslythrough any means whatsoever.
10. **Stealing,concealing,ordamagingcomputersourcecode:**Ifitexploits,hides,damagesoralters,orallowsanother person to steal, hide, damage, ormodify any computer source code used for a computer resource intended to cause harm. [Inserted vide ITAA, 2008].

Explanationofthewordsusedincompliancewithsection43[2]

1. **"ComputerContaminant"**meansanyvarietyofcomputerinstructionswhicharedesigned(a)toalter,delete,capture,transmit data or program within acomputer, acomputer system, or acomputer network; or (b) tocapture illegally by any means the regular activity of a computer or a CNW.
2. **"ComputerDatabase"**meanstherepresentationofdata,information,facts,concepts,orinstructionsintext,images, audio, video that are prepared or prepared in a formalized manner or generated by a computer, computer system, or a computer network and intended for use in a computer, a CS or a CNW.[3]
3. **"Computer Virus"**means any computer instruction, information, data, or software that damages, destroys and diminishes,oradverselyaffectstheoutputofacomputerresourceorattachesitselftoanothercomputerresourceand operates when a program, data, or instruction is executed or any other event occurs in that computer resource.
4. **"Damage"**means the degradation, alteration, elimination, addition, modification, or reorganization of any computer resource by any means.
5. **"Computer Source Code"**means the listing in some type of programs, computer functions, design and layout, and software analysis of computer resources.

Compensationforfailuretoprotectdata[43A,InsertedvideITAA,2008]

This section provides that if an entity is negligent in carrying out and maintaining fair security practices and procedures, processing,handling,orhandlinganyconfidentialpersonaldataorinformationinacomputerresourcethatitowns,manages,or operates, andtherebycauses wrongful loss or benefit to any person, that entity shall beliablefor damages byway of compensation.[4]

ExplanationofthewordsusedinSection43A

1. **"BodyCorporate"**meansanycompanyandinvolvementinacompany,soleproprietorship,orothergroupsof individuals engaged in commercial or professional activities.
2. **"Reasonable SecurityPracticesandProcedures"**meanssecurity practicesand proceduresdesigned to protect suchinformationfromunauthorizedaccess,harm,usage,alteration,exposure,ordisruptionasmaybeprovidedforin anagreementbetweenthepartiesorasmaybeprovidedforinanylawforthetimebeingineffectandintheabsence ofanyagreementoranylaw,suchreasonablesecurityasmaybeprovidedforinanagreementbetweentheparties.[5]
3. **"Sensitive Personal Data or Information"**means confidential information as may be recommended by the Central Government in collaboration with such professional bodies or organizations as it may deem necessary.[6]

Penaltyforfailuretoprovideinformation,returnorreport(Section44)

Thissectionprovidesforthefollowingpenaltiestobeimposedonapersonwhohastocomplywithcertainlegalobligationsunder this Act, the rules or regulations made thereunder:

1. Punishmentforfailuretoincludeanypaper,returnorreport toCCA or CA.For eachsuchloss, heshallbeliabletoa penalty not exceeding 1,50,000.
2. Penaltyfor failuretoreturnorfurnishrecords,books,or other documents within adefinedtimeperiod.Heshall beliable for a penalty not exceeding 5,000 for each day on which such failure continues.
3. Penaltyfor failuretomaintainbooks of accounts ordocuments.Heshallbeliableforapenaltynotexceeding10,000 for each day on which the failure continues.

Penaltyforcontraventionofrulesorregulations(Section45)

Thissectionprovidesthatifapersoncontravenesanyoftherulesorregulationsimposedpursuanttothis Actforwhichnopenalty has been levied, the person concerned shall be liable to pay compensation not exceeding 25,000 to the affected person.[7]

Powertoadjudicate(Section46inTheInformationTechnologyAct,2000)

1. Inordertodecide,inaccordancewiththis Chapter, whetherapersonhas committedaninfringementof anyprovision ofthisAct orofanylaw, regulationorordermadethereunderwhichmakes himliabletopaypenaltyorcompensation, theCentralGovernmentshall,subjecttotheprovisionsofsubsection(3),appointanyofficernotlessthantheDirector oftheGovernmentofIndiaoranequivalentofficeroftheGovernmentoftheStatetobeanadjudicatorfortheconduct ofaninvestigationinthemannerspecifiedbytheCentralGovernment.[8][(1A)Theadjudicatingofficernamedpursuanttosubsection(1)shallexercisejurisdictiontoadjudicatemattersinwhichtheclaimforinjuryordamagedoesnotexceedfive crores:giventhatthejurisdictioninrespectoftheclaimforinjuryordamageexceedingfivecroresiswiththe competent court.]
2. Theadjudicatorshall,afterprovidingthepersonreferredtoinsubsection(1)afairopportunitytomakerepresentations in thematter and if he is satisfied, on such an examination, that theperson has committed the violation, imposesuch penalty or grant such compensation as he considers necessary in accordance with the provisions of that section.[9]
3. Noindividualshallbeauthorizedasanadjudicatorunlesshehassuchexperienceinthefieldofinformationtechnologyandlegal or judicial experience as may be prescribed by the Central Government.
4. Where more than one adjudicating officer is authorized, the Central Government shallby regulation, determine the matters and places in respect of which those officers shall exercise their jurisdiction.
5. Eachadjudicatorshallhavethepowersofacivilcourtbestowedonthe CyberAppellateTribunalpursuanttosubsection (2)ofsection58,and-
   - (a)anyproceedingsuntilitshallbeconsideredtobejudicialproceedings withinthescopeofsections193 and 228 of the Indian Penal Code (45 of 1860);
   - (b)shallbedeemedtobeacivilcourtforthepurposesofsections345and346oftheCodeof CriminalProcedure, 1973 (2 of 1974);
   - [(c)shallbeconsideredtobeacivilcourtforthepurposesofOrderXXIoftheCodeofCivilProcedure,1908(5of1908).

Section47inTheInformationTechnologyAct,2000

Factors tobetakenintoaccountbytheadjudicating officer. -Whiledeterminingtheamountofcompensationreferredtointhis Section, the adjudicating officer shall take due account of the following factors, namely:

1. theamountofunfairadvantageobtained,whereverquantifiable,asaresultofthedefault;
2. thesumofdamagessustainedbyanyindividualasaresultofthedefault;
3. therepetitiveaspectofthedefault.[10].

UNIT-3

FeaturesofPatentLaw(IndianPatentAct)

The history of inventionsbegin with the invention of wheels but patents (An exclusive right to owner to protect his invention andprohibitsothersfromusingit)were granted in the15thCenturyonly. Initiallypatentsweregranted fornaycommon research andinventionsitresultedinhugedissatisfactionamongstpeopleandfinallyresultedintheformationofalegalproceduretoprotectinventionandawarditodeservingcandidates, it isknown as Paten Lawor Patent Act. Thislaw declared all the non-inventions illegal.The Patent Law was first introduced byAtateof Venice in 1474.The first Patent Act of the U.S. Congress was passed on April10, 1790, titled “An Acttopromote theprogressofusefulArts.” The first patent was granted onJuly 31, 1790 to Samuel Hopkins for a method of producing potash(potassium carbonate).

The history of Patent law in India traces back to 1911 when the Indian Patents and Designs Act, 1911 was passed. The present PatentsAct,1970 came into force in the year 1972, amending and consolidating the existing law relating to Patents in India. The Patents Act, 1970wasagain modified by the Patents (Amendment) Act, 2005and it was extended to all fields of technology including food, drugs, chemicalsandmicroorganisms. After theamendment,theprovisions relatingtoExclusiveMarketingRights (EMRs)havebeen cancelled, anda provisionforenabling grant of compulsory license has been introduced. The provisions concerning to pre-grant and post-grant opposition havebeenalsointroduced.

- **Bothproductandprocesspatentprovided**
  - The Law permits to patent any invention that is new,useful to the society, has commercial application andinventivestep. The patent is granted for product as well as process. Roche India Pvt Ltd, the Indian arm of Swissdrugmaker FHoffmannLaRoche,gotitsfirstPatentinIndiaforitsbiotechdrugPegasys(Peinterferonapha-2a).Patentforprocesswas provided to “A process of making rare earth doped optical fibre”
  - Amereadmixture,methodofagricultureorhorticultureandplantsandanimalscannotbepatentedunderthisAct

- **Requirementforapplication**
  - Anapplicationforpatentshouldcontaincompletedescriptionoftheinvention(alsoknownaspatentspecification).
- **Examinationonrequest:**
  - Afterfilingtheapplicationforapatent,arequestforexaminationisessentialtobemadeforexaminationoftheapplicationbytheIndian Patent Office.

- **Bothpre-grantandpost-grantopposition:**
  - The patent can be opposed by any person within six months from the publication of the patent application. Thisisknown as Pre grant opposition. The invention can be challenged even after it gets patent, but the oppositionshouldcome within 12 months from the publication of the grant of the patent.
- **TermofPatent**
  - Thetermofpatentineverycategoryinindiaistwentyyearsfromthedateoffilingthepatentapplication.Incase ofapplicationsfiledthroughthePatentCooperativeTreaty(PCT),b theterm of twentyyears eginsfromtheinternationalfilingdate.
- **RenewalFee:**
  - Thepatenteehastopayrenewalfeetokeepthepatentalive.
- **PatentofBiologicalMaterial**
  - Iftheinventionusesabiologicalmaterialwhichisnew,itisessentialtodepositthesameintheInternationalDepositoryAuthority(“IDA”)before filing of the application in India in ordertosupplement thedescription.Publication ofapplicationsafter 18 months with facility for early publication.
- **RightsconferredonthePatentee:**
  - Theactgivesexclusiverightstothepatenteetomanufacture,market,sell,assignandlicensehispatentandatthesametimeprohibitothersfromdoingsoforalimitedperiodoftime.Italsoprovidesreliefsagainstinfringementsintheformof injunction andcompensations.
- **Compulsorylicensing**:
  - Theactalsoensuresthatpatenteedoesn’tmisusehisrightsandalsothatpatentsdonotpreventtheprotectionofpublichealthandnutrition,bythewayofCompulsoryLicensing.Undersection84ofIndianPatentAct,compulsorylicensesaregranted
    - Topreventthemisuseofpatentasmonopoly
    - ToMakeprovisionsforcommercialexploitationofthepatent(IfgovernmentfeelsthatpatentisnotavailabletopuBlic at an affordable price, or reasonable requirements of public have not been satisfied.
    - Totakecareofpublichealthinindia.
  - **Assignment**
    - Thepatenteecanassignhisrightstoanyotherperson.Assignmentisavailableinthreeform-legalassignment,equitable assignment and mortgages

TRADEMARKLAW:

The historyof trademarklaw to the cyberspace canbe associatedwiththe creationof the WorldWideWeb(www)whichcertainlycreateda linkof trademarklawwithInternetdomainname disputes.Andithascreatedabuzzamongstusersascommercialization of the Internet medium. Thousands of businesses haveestablished storefronts on the Internet todisseminate marketing literature, offer customer service, and sell goods andservices online. Not surprisingly, due to thiscommercialization factor, there is an increasing relation between trademarklaw and domain names.1 As a consequence,the following dynamic growth of the World Wide Web has issued newchallenges to the intellectual property consultantsconcerningtrademarkinfringement.Fortrademarkowners,internetisaprofitableplatform,butincertaincases,itturnsout to be problematic intheir business growth. These trademark ownersoften have to deal with certain

domainnamedisputesinflictedbythethirdpartylikecybersquattingetcbutinIndia,wepersaydonothaveanyDomainName

Protection Law so the cases relating to cyber squatting are decided under Trade MarkAct, 1999. Under the currentlaw,section 292 provides for the protection of registered trademark and the protection for unregistered trademark hasbeenprovided in section 323 . However, the act is silent on the protection for trademarks infringement in the cyberspace.Themajorityofdomainnamedisputesseemtoinvolvetrademarksasitissubmittedthatthedisputeariseswiththeregistrationoruseofthedomainname whichinfringesanylegallyrecognizedright,suchasanytrademarkright,commonlawrightinpassingoff,oranyotherrightforthatmatter.Astrademarklawsareterritorialinnaturebutinternetintheglobaldomainso the dispute involving bad faith registrations are typically resolved using the UDRP (UniformDomain Name DisputeResolution Policy) process which is developed by the ICANN. Under UDRP, WIPO happens to bethe leading ICANNaccredited domain name dispute resolution service provider whichwasestablishedas a tool forpromoting the protection,dissemination, and the use of intellectual property throughout the world.4 Since TRIPSagreementprovidesforonly1MurugendraB.Tubake;USandIndianTrade Marks Law:AComparison; PLFebruary S-1 Introduction (2012).

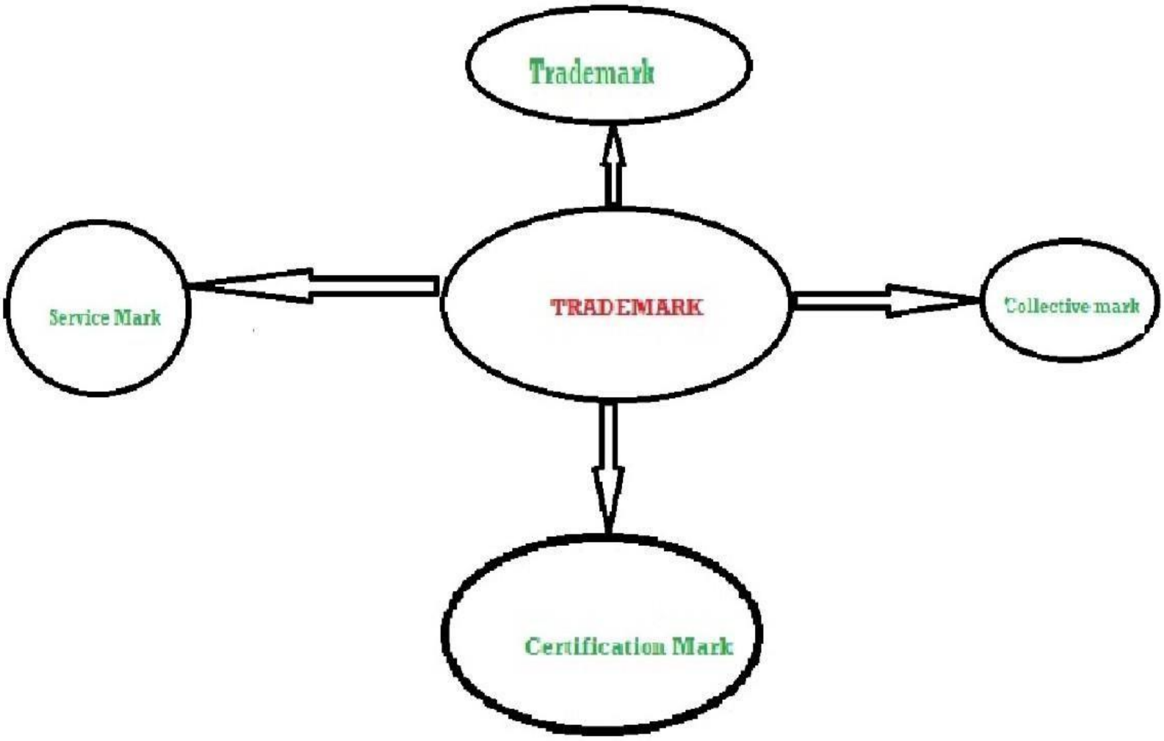
2TrademarkAct,1999,IntellectualPropertyLaws,UniversalLawPublishing,(2015).3Ibid.4TheUniformDomainName DisputeResolutionPolicyandWIPO;©WorldIntellectualPropertyOrganization,(2011).OpenAccessJournalavailableatjlsr.thelawbrigade.com41JOURNALOFLEGALSTUDIESANDRESEARCHINTELLECTUALPROPERTY RIGHTSLAWREVIEWVolume3Issue3[June2017]minimumstandardsso,thereexistssimilarityuptosomeextentinthedomesticIPlawsandexcepttheseprinciplesthereareharddlyanylawswhichareuniform,andasaresultofwhichthereexist some advantages and disadvantages of nation over other nations IP laws.

Trademarks

Trade●marks are the marks that are external to the goods to make the public identify a certain quality and image relatedwiththatproductorservice.Itisanimportantwayof promotinggoodwillofthe companyororganisationwithitsclientsorcustomers.

Ithasalegalprotectiontopreventothersfromusingit.FewexamplesoftrademarksareTata,godrej,IIMetc.

TypesTrademarks:
Trademarkscanbeclassifiedinto4types:



1. **Trademark** –
   It is a mark which includes any word, name, symbol, or any combination which is used in commerce to identifyanddifferentiate the products of a manufacturer from products of others. In short, Trademark is a brand name.
2. **Service Mark** –
   It is a mark which includes any word, name, symbol, or any combination which is used in commerce to identifyanddifferentiate the services provided by one provider from services provided by others. It is used in servicebusiness.
3. **Certification Mark** –
   Itisamarkwhichincludesanyword,name,symbol,oranycombinationwhichisusedincommercebyotherpersonswithowner's consent andcertifies them regional,material,modeofmanufacture, or other characteristics of owner'sgoods.
4. **Collective Mark** –
   It is a mark which includes any word, name, symbol, or any combination which is used in commerce by membersofan association or group or organization.

Advantages of Trademarks:
TheadvantagesofTrademarksareasfollow:

- Itprovidesadditionalrevenuestreamtotheowner'sthroughlicensing.

- Itprovidesincreasedcustomerrecognitiontothebrands.
- Itprovideslegalprotectiontothecompanyusingaparticulartrademark.

- Itpromotesthegoodwillofthebrand.
- Itencouragesparticipationfromotherbrandsthroughco-branding,brandextension.

Copyright:

Copyright is a legal term describing ownership of control of the rights to the use and distribution of certain works of creativeexpression,includingbooks,video,motionpictures,musicalcompositionsandcomputerprograms.Historically,copyrightlawhasbeenenactedto balancethedesireofculturestouseand reusecreativeworks --thuscreating"derivativework" --againsttherightsofauthorsofart, literature, musicand thelike to monetize their work by controlling who can make and sell copies ofthe work.

To strike this balance, the exclusivity of control is almost always restricted to a set period of years, after which a copyright-protectedworkreverts to the public domainand may be freely used.

Whoisacopyrightowner?

The copyright holder is often a company or corporation. If a work is created as a component of employment -- work for hire -- thenthecopyright for the work defaults to the employer.

Copyrightownershipisboundedbytheterritoryofthejurisdictionin whichithasbeengranted --acopyright grantedbytheUnitedStatesisvalidonlywithin that country, for example -- as well by certain specific exceptions. Much of international copyright law was broughtintorelativeconformitywiththeBerneConventionfortheProtectionofLiteraryandArtisticWorks -- usuallyreferredtoastheBerneConvention --in1886,withnumeroussubsequentrevisionsoverthedecades.TheWorldIntellectualPropertyOrganizationCopyrightTreaty -- alsoknownastheWIPOCopyrightTreatyorWCT--wasadoptedin1996tocoverinformationtechnologyandtheinternet,elementsnotdirectlyaddressed in the Berne Convention.

An important shift in copyright legislation that appeared in the Berne Convention was the move to make copyright protection automatic.Inmostcountriestoday,creatorsdonotneedtoregisterorapplyforcopyrightprotectionofawork.Rather,theauthorofaworkisimmediatelyentitled toall copyrights of the work until those rights are explicitly disclaimed or the copyright expires.

Before1989,UnitedStateslawrequiredtheuseofacopyrightnoticetoassertthatcopyrightwasbeingclaimed.Thecopyrightsymbolortheword *copyright*hadtobeplacedsomewhere withintheprotectedwork,alongwiththeyeartheworkwascreatedorpublished.

Whatisthedurationofcopyrightprotection?

Afterawork'scopyrightexpires,theworkfallsintothepublicdomainandcanbeusedatnocostandwithoutrestriction.Theoriginalcopyrighttermwassetat14 years, with theoption torenewforanother14 years. Thattermwasdoubled in1831to28 yearsplusone28-yearrenewal.

DisneyCorp.isthebestknownofagroupofpowerfulcopyrightholdersthatbenefitfromlongercopyrightprotectionterms. Disneyhasbeena drivingforce to extend U.S. copyright protection for its iconic mouseand supported changesto copyright terms inthe U.S.,includingthefollowing:

- **CopyrightActof1976**,whichextendedcopyrightprotectionto75yearsorthelifeoftheauthorplus50years;and
- **Copyright TermExtension Actof1998**,alsocalledtheMickeyMouseProtection Act,whichextendedthetermto120years or the life of the author plus 70 years.

Under current copyright law, Disney's copyright on the original version of Mickey Mouse portrayed in *Steamboat Willie*in 1928 is settoexpire in 2024.However, subsequent versions of theDisney mascot, as well as most ofDisney's other characters, will still be protected.

Whatisthedurationofcopyrightprotectionundercurrentlaw?

Under current lawin the U.S., works created after Jan. 1, 1978, are afforded copyright protection for the life ofthe authorplus anadditional70years.Foranonymous,pseudonymousandcorporate-ownedworks,acopyrightlasts95yearsfromtheyearofitsfirstpublicationoraterm of120yearsfromtheyearofitscreation,whicheverexpiresfirst.

Copyrightdurationandpublicdomain

The notion of protecting publishers from unauthorized third-party sales of copies of their books dates back to the 1709 Statute of AnneinBritain,alawthatgavepublishersexclusivepublishingrightsforafixedperiod,afterwhichtheirworkcouldbeproducedandsoldbyothers.In the United States, the first legislation along these lines appears in the U.S. Constitution, in Article I, Section 8, Clause 8, where the so-calledCopyright ClausegivesCongresstheauthoritytoenact laws"securingfor limited TimestoAuthorsand InventorstheexclusiveRightt o theirrespective Writings and Discoveries."

Both these laws, along with current copyright legislation worldwide, call for protected works to enter the public domain after thecopyrightlaw's stipulated term has passed. Works in the public domain may be used, copied and distributed with no restrictions undercopyrightlaw.

7 ways to prevent software piracy

1. License keys
2. Antipiracy software
3. Print/copy restrictions
4. Streaming protections
5. Copyright symbol
6. Antipiracy incentives
7. Demo or trial version

SOURCE: MICHAEL COBB AND MIKE ROTHMAN;
ART: VECTORMINE/ADOBE STOCK
©2021 TECHTARGET. ALL RIGHTS RESERVED

Including acopyrightsymbolinallwebsitecontentcanhelpdefendagainstlegalassertionsofunintentionalcopyrightinfringement.

Whataretheexceptionstocopyright?

Noteveryexpressionofanideamaybecopyright-protected.Copyrightdoesn'tprotectthefollowing:

- productnames;
- titlesofworks,suchasbooktitles;
- namesofbusinessesandorganizations;
- pseudonyms,includingcomputerhackernyms;
- slogans,catchphrases,mottosandshortadvertisingphrases;and
- listsofingredients,suchasonproductlabelsorasusedinrecipes.

Somethingsonthislist,suchasproductnames,maybeaffordedprotectionundertrademarklaw.

Fairuse

Even whena work isprotectedunder copyright law,thelawdefinesa categoryof exceptions.In thesecases,copiesofworksmaybeusedeven when the copyright holder has otherwise restricted use.

Fairuse,knowninsomeotherinternationaljurisdictionsas*fairdealing*,isthejudicialdoctrinethatpermitstheuseofcopyrightedmaterials whenthepurposeservesthepublicinterest.

Themostcommonfairusesforcopyrightedmaterialsincludethefollowing:

- **Criticismandcomment**fairusesallowreproductionofacopyrightedworkforthepurposeofcriticizingorcommentingonthework. Itisinthepublic'sinterest to haveaccesstocriticalreviewsof works,andinconsideringtheseworks, thecriticmayincludeshort excerpts ofa work in order to illustrate a point being made.
- **Parody**fairuseisanothercommonfairuse,wherepartsoftheworkarereproducedinanewwork.
- **Educational**fairusepermitsuseofmaterialsinface-to-faceteaching,forscholarshipandforresearch.
- **Publicgood**fairuseincludesexceptionsforallowinglibrariestomakeBraillecopiesofbookstheyown.
- **Noncommercial**fairuseincludesexceptionsliketheonesthatpermitrecordingradioortelevisiontransmissionstowatchinanoncommercialsettingormakingcopiesofworkslike softwaretoavoidproblemsintheeventoftheoriginalworkbeing stolen,lostordamaged.

Conceptually,fairuseisarefinementofthebasicbalancecopyrightstrikesbetweenauthorandcivilinterests.

Itisimportanttonote,though,thatwhatcountsasfairuseisgenerallynotwelldelineatedincopyrightlawsaroundtheworld.IntheU.S.,thelawlistsfourbasic guidelines that courts may use in lawsuits where infringement is alleged:

1. **Commercialornoncommercial.**Isthepurposeandcharacteroftheuseprimarilynonprofitandtofurthereducation,oris itforprofit?Nonprofit,noncommercialeducationalusesaremorelikelytobeconsideredfairuse.
2. **Natureofthework.**Istheprotectedworkafactualwork,whichisentitledtolessprotection,orisitapurelycreativework? Factualworksincludefactsthatmaybeofpublicvalue,andsincetheyarefacts,theyrequirelesscreativeworktocreate.
3. **Amount and substantiality of the portion of the work used.** How much of the protected work is being used, andhowcentralisittothework?Usesofquotesandothershortexcerptsaremorelikelytobetoleratedthanusesofextensiveportionsof thework.
4. **Effectof the use uponthe potential market for the work.** Howlikelyis it that the useisintended toavoid paying forthework? For example, makinga copy ofa software programto install it onanothercomputeris not fair use, while making abackupcopytoavoidbusinessdisruptionduetotheft,lossordamageisusuallyconsideredafairuse.

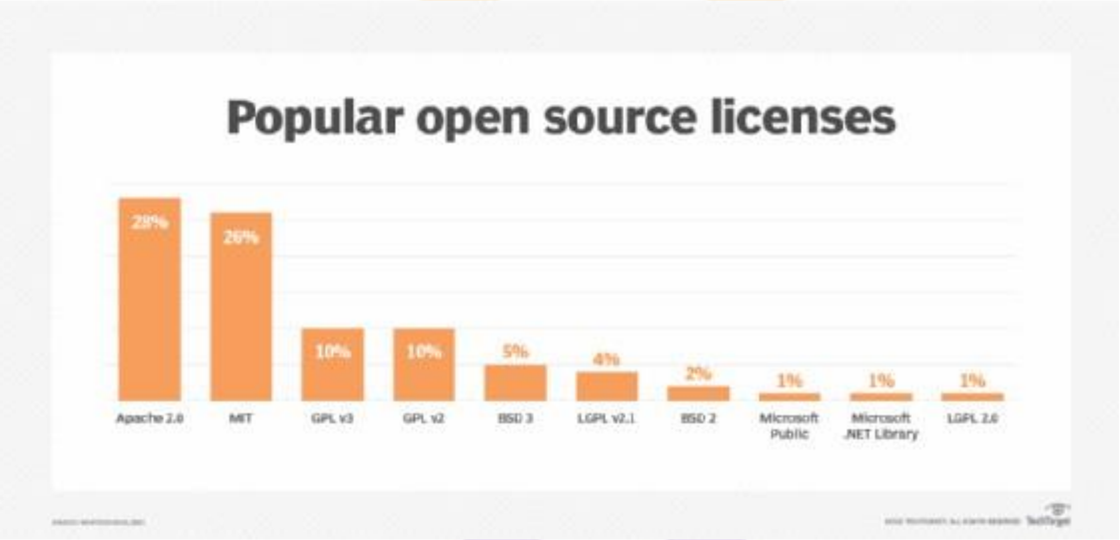
In the world of popular music, the boundaries of fair use have been tested as a result of the use of samples, or short snippets of copyright-protectedsoundrecordingsinnewworks.Clearprecedentshavenotbeenestablishedbecausecourtdecisionshavetakenunpredictableturns.

A2005 decision in the 6th District Court in the U.S. held that copying even as fewas three consecutive notes could constituteinfringement.Other cases have revolved around whether permissions must be obtained for portions of a work that are sampled, for theunderlying song orboth. Commercial musicians can buy clearances to sample works, meaning that whether that sampling could be allowedunder fair useprovisions is simply not tested.

Copyleft

Aninterestingexceptionofsortstocopyrightisaconceptoriginallychampionedby RichardStallmanandtheFreeSoftwareFoundation, whichcreatedcopyleftasameansofeffectivelystrippingmostcopyrightrestrictionsfromaworktoallowfreeuse,includingcopyingofthe material,whileretainingcontroloverhowthematerialisshared.

Underthecopyleft,derivativeworkscreatedusingthatoriginal work mustalsobegivencopyleftprotection.Morebroadly,this approachisknown as *free licensing* and is considered a form of open sourcelicensing.

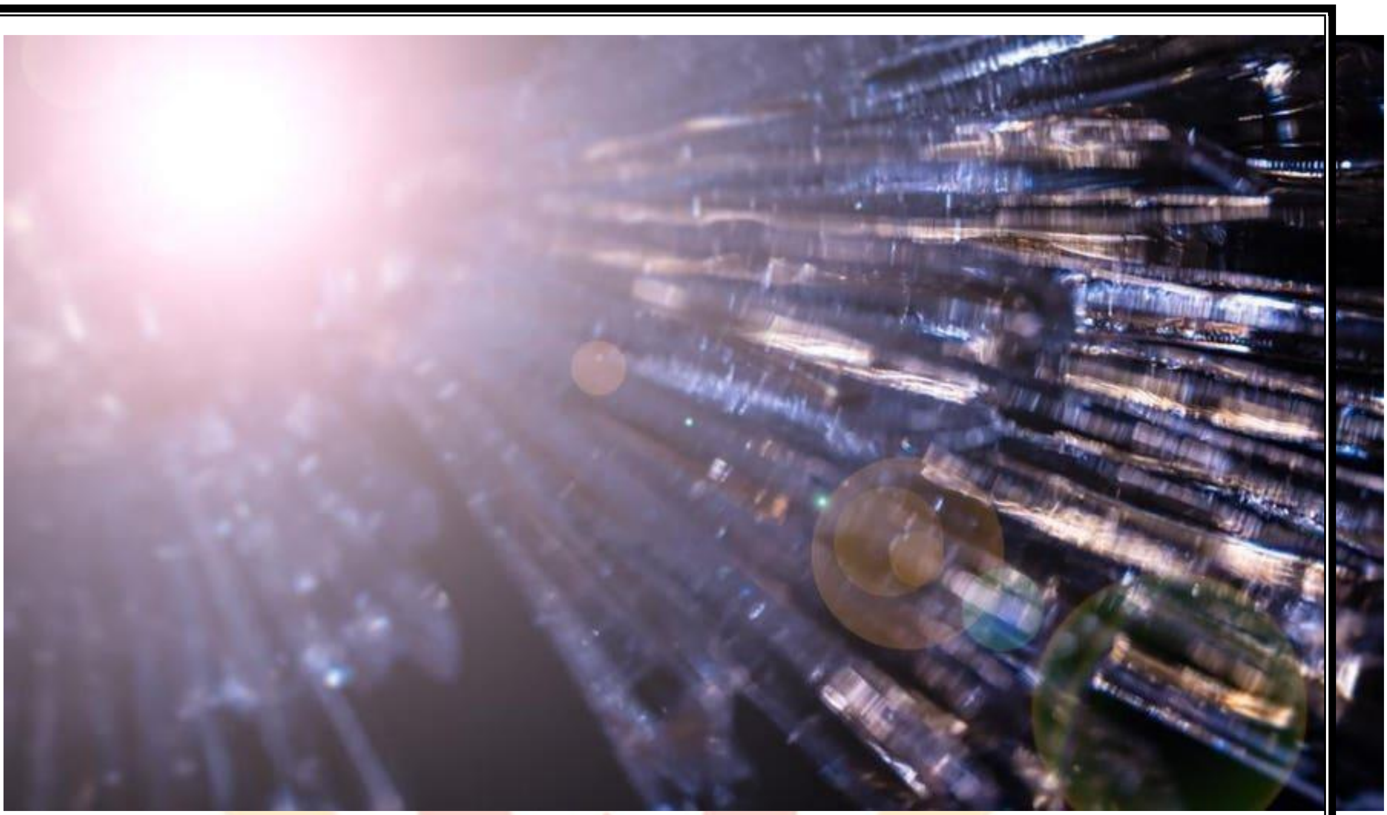


Materialpublishedunderopensourcelicensesmaybefreelycopied,modified,sharedanddistributed,aslongastheoriginallicenseisappliedtothedistributed material.Whenusedforpublishingsoftware,thecopyleftlicensealsorequiresthatsourcecodebeincludedormadeavailable whenmodifiedsoftwareispublished.

CreativeCommons

In2001,CreativeCommons,anonprofitorganization,wascreatedtofacilitateseveralkindsoflegalsharingsothatworkscouldbefreely reusedbutincontextsthatarecontrolledbythecopyrightholder.WorkscoveredunderCreativeCommonslicensesareaggregatedatcreativecommons.or g.

TrademarkVs.CopyrightVs.Patent:What’sTheDifference?



Entrepreneurswhoownatrademark,copyrightorpatentforaproduct ortechnologyhaveanadvantageovertheircompetitors.But theprocess for obtaining these intellectual property protections can be long and complicated. Before you start the process,it isimportanttolearnaboutthedifferencesbetweenatrademark,copyrightandpatent.We'llwalk youthrough howeach canhelpprotect your company's intellectual property, what exactly they protect and where you need to apply.

DefinitionsofCopyright,TrademarkandPatent

CopyrightsareregisteredbytheU.S.CopyrightOfficeattheLibraryofCongresswhiletheU.S.PatentandTrademarkOfficewillgrantpatent s and register trademarks.

Hereisabriefexplanationofeachtypeofintellectualproperty.

Trademark

Atrademarkcanbeaphrase,wordordesignthatidentifiesyourcompanyanditsgoodsorservices.Atrademarkcan helpdistinguishyoufromyourcompetitorsandpreventothersfromusingyourmark.Therearestate-levelandfederal-leveltrademarks,eachwith its own registration process.

Patent

A patentisa grantedpropertyrighttothecreator(s)of a new,uniqueandusefulinvention,discovery orprocess.Patentsallowyoutobarothersfrommaking,usingorsellingyourinvention.Therearethreemaintypesofpatents:utility,designandplant.

Copyright

A copyright protects original works of authorship including songs, books, movies, articles and much more. The key is thatthework must exist on a physical ordigital medium, such as paper, filmora digital file. A copyright gives you the exclusive righttousea work in a varietyof ways: you can reproduceit,sellordistributecopies, display it,perform it, orcreateotherworksbasedonyourcopyrightedwork.Copyrightsareautomaticuponcreationoftheoriginalwork,butregistrationisrecommendedsothatthecopyright claim is part of the public record.

AdvantagesofObtainingCopyright

A copyright is granted the moment you create an original work in a tangible or fixed form. It's automatic. Butunregisteredworks may be difficult to prove in the case that someone else uses or steals your work. And you can only file acopyrightinfringementlawsuitifyourcopyrightisregistered.That'swhywerecommendregisteringyourworkwiththeU.S.CopyrightOffice to make your copyright claim public record.

AdvantagesofReceivingaFederalTrademark

Receiving a trademark means your competitors can not register the same, or a deceptively similar, trademark in the sameclassofgoodsorserviceswhereyourtrademarkisregistered.Registrationcreatesapublicrecordofyourtrademarkownershipandit allows you to use the ® symbol, helping establish legitimacy and trust with your customers and ward off counterfeiters. Afederaltrademark also gives you additional ways to enforce the mark and paves the way for registering your mark in othercountries.

AdvantagesofHavingaPatentApproved

Innovationscantakeyearstocreateandareoftenexpensive.Receivingapatentensuresyou'llhavetheopportunitytoprofitfromyourhardwork.Apatentmeanstheinventionsandanyrelatedprocesses cannotbecopied,madeorsoldunlesspermissionisgivenby the inventor.

CopyrightVs.TrademarkVs.Patent

Hereisabriefoverviewonhowyourcompanymightuseacopyright,trademarkorpatent.

	Trademark	Patent	
Definition	Atrademarkcanbeaphrase,wordordesign—orall three—thatdescribeswhatyourcompanydoes or sells. Having a trademark can help separate youfromyourcompetitors	A patent grants property rights to the creator(s) of anew, unique and useful invention,discoveryorprocess.Thereare threetypesofpatents:utility,design and	Acopyri htisa original wo ksofa

	Trademark	Patent	
		plant	
Example	Nameexample:McDonald’sSloganexample:I’m Lovin’ItLogoexample:Thegolden arches	ThedesignoftheiPhone;BlueToothdata transferringtechnology;Keurig’sK-Cuppod	Logos,illu tration copy,pho tograp indiv
Length of protection	Can last forever, but you must file periodic maintenanceandrenewalpaperworkstartingfive years after registration	Typically20years	Ingenera Life o madefor ire(wo that esthe publicati or12
Application cost	Initialfeeof$250perclassofgoods/services	Initialfeeofatleast$80,plusfeesforsearch and examination fee, depending on size of company	

Howdocopyrightswork?

Copyright protects "original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels,movies,songs, computer software, and architecture,"accordingto the USPTO.

Aworkisautomaticallyprotectedbycopyrightfromthetimeitiscomplete.Theauthoroftheworkcanclaimcopyrightprotectionbyaddingthe copyrightsymbol (©) or the word *copyright* and their name and the year the work was created.

Creators can secure greater protection for their work byregistering it with the U.S.Copyright Office. This requires submittinga copyoftheworkandacopyrightregistrationfee;workscanberegisteredonlineforaslittleas$35,andgroupsofworks,suchasarticlesinaperiodical,canbe registered as well.

Copyrightstatusisprotectedfromtheinitialcreationorregistration.

Howdotrademarkswork?

Trademark owners can register trademarks with theUSPTO toprotect their brand, logoor slogan as it relates totheirproduct.Thisprovidesconfidence to consumers when buying a trademarked product, such as Coca-Cola® or The Happiest Place on Earth®.

Gettingtrademarkregistrationismorecomplicatedandmoreexpensivethancopyright.ApplicationfeeswiththeUSPTOstartat$250andmayrequire trademark searchesand other processes; applicantsusually work withanattorney to complete the registrationprocess.

Acceptanceandregistrationofatrademarkarenotguaranteed,butonceatrademarkisregistered,itmustbeactivelyusedbytheowner.Trademark protection can persist indefinitely ifthe owner continuestouse it andrenews the registration every10 years.

Howdopatentswork?

Governmentsgrant patentsto inventors to enable inventors toprofit fromtheirinnovations. Apatented invention must benovel, nonobviousanduseful, and if the USPTO determines that is the case, the inventor hasan initial term of protection lasting up to 20 years.

Patentscan'tberenewed.Buttheymustbemaintainedbypayingmaintenancefeesduringthepatentterm,orelsethepatentedinventionlosespatentprotection.

The USPTO evaluates patent applications; the patent application process includes numerous fees, which depend on the type of patentandother factors. The process is best navigated with a patent attorney, who can assist in submitting the application and responding toadditionalrequirements where needed.

Howisdigitalrightsmanagementusedforcopyrightcontrol?

Digitalexpressions,suchase-booksandmusic,areprotectedundercopyrightjustastheirtraditionalbookandcompactdisccounterpartsare. Controllinginfringementandunauthorizedreproductionofdigitalworksisconsiderablymoredifficultthanhard-copyproductsthatrequire printingandphysicaldistribution.

Copyrightprotectstheseworksandcanbeusedasthebasisforlawsuitsafterthefact,butcorporationshaveembracedtheideaofusingdigitaltechnologiesto protect digital works.

Therearetwobasicapproachesusedintypicaldigitalrightsmanagement(DRM)products:

1. Individualcopiesofthedigitalproductareencryptedandcontainthecodenecessarytoprotecttheiruse.Theprotections usedtopreventunauthorizedduplicationofcommerciallydistributeddigitalvideodiscsareexamplesofthisandrelyon safeguardsbuiltintoDVDplayerstopreventtheuseofpiratedcopies.
2. Acentralizedrightsmanagementserverchecksauthorizationsattimeofuseandlocksorunlocksdigitalcopiesaccordingly. Thisallowsfiner-grainedcontrolandbetteroveralluseaccountingbutrequiresaninternetconnectionbeforeeachuse.

Thereare,insomeDRMsystems,additionalcontrolsenforced.BooksreadintheAmazonKindleecosystem,forinstance,canbehighlightedwithinthe context of the present copy, but copyingtext displayed ina Kindlereader to the clipboardofthe operating systemisn't allowed.

ThisDRM-imposedrestrictiononcuttingandpastingis,criticshavenoted,arestrictionthatgoesbeyondtherightsprovidedundercopyrightlaw,wherethat cuttingandpastingmight well fall intotherealmof fair use.Not beingabletomakebackupcopiesofDVDsisanother casewhereuse ofawork isallowed under copyright but may be prohibited by the DRM system a corporation has opted to use.

DigitalMillenniumCopyrightActof1998

TheDigitalMillenniumCopyrightAct(DMCA)of1998includesastipulationthatmakesitacriminaloffensetoreverse-engineerDRM systems, even iftheaimistotake actions that are allowed under that samecopyrightlaw. Manufacturers of goods, suchas farmtractorsandcars,that one wouldn't normally associate with copyright protectionshave asserted that the DMCA reverse-engineering provision appliestosoftwareused in embedded systemswithintheir products.Thus,third-partyattempts to understandthose systemsare criminal offenses, not becauseofcopyrightinfringement,butsimplybecauseresearchontheworkingsofDRMsystemsisillegal.

AnumberofprosecutionsandthreatenedlegalactionshavebeenmountedsincetheDMCAwasenacted.ApartiallistoftheseismaintainedbytheElectronic Frontier Foundation.

Fairuseforsecurityresearch

InOctober2016,theLibraryofCongresstemporarilyauthorizedsecurityresearcherswhowere"actingingoodfaith"toconductsomekindsofresearchon consumer devices so longas the research did not violate other laws, such asthe Computer Fraudand Abuse Act.

Thereisafour-parttestforwhetheranygivenresearchfallsundertheexemption:

1. Thecomputerprogrammustbelawfullyacquired.
2. Theactionstakenmustbe"solelyforthepurposeofgood-faithsecurityresearch."
3. TheresearchmusttakeplaceafterOct.28,2016.
4. Whilenottechnicallyarequirement,theauthorizationimpliesthatresponsibledisclosureisanimportantelementinestablishing thatthe work was done in good faith.

Goodfaithiscircularlydefinedasbeing"solely forthepurposesofgood-faithtesting"butisalsoexplainedto meanthework can't bedone"in a manner that facilitates copyright infringement."

Onlyresearchconductedwithprimarilyconsumer-orientedproductsfallunderthisauthorization.

Seewaystoprotectintellectualpropertyandtradesecrets,secureagainstinsiderthreatsandbestpractices.

ThiswaslastupdatedinDecember2021

ContinueReadingAboutcopyright

- Howtopreventsoftwarepiracy
- Thefutureofopensourcelicensesischanging
- 5commonopensourcesoftwarelicensesyouneedtoknow
- 5factorsforusingopensourcecodeinproprietarysoftware
- U.S.CopyrightOffice:Registeringawork

RelatedTerms

governance,riskandcompliance(GRC)

Governance,riskandcompliance(GRC)referstoanorganization'sstrategyforhandlingtheinterdependenciesamongthefollowing...See completedefinition

riskavoidance

Riskavoidanceistheeliminationofhazards,activitiesandexposuresthatcannegativelyaffectanorganizationanditsassets.Seecomplete definition

totalrisk

Totalriskisanassessmentthatidentifiesalltheriskfactorsassociatedwithpursuingaspecificcourseofaction.Seecompletedefinition

Issoftwareprotectedbycopyrightsorpatents?

Computersoftwareorprogramsareinstructionsthatareexecutedbyacomputer
Softwareisprotectedundercopyrightlawandtheinventionsrelatedtosoftwareareprotectedunderpatentlaw.

SourceCodeandObjectCode

Computer software are instructions that formsourcecode and object code. Softwaretakes a lot of skill, time, and labor to develop them, soit is natural that you want to protect all your hard work. Computer programs can be copied and used by unauthorizedpersons.Youractualsoftwareandappsourcecodemaybeprotectedundercopyrightlaw,.Theconceptsandinventions related to software may be protected under patent law.

COPYRIGHTPROTECTIONS

Copyright Law defines computer programs as literary work, and as suchis protectableunder copyrights. For example, computerprograms aresets of instructions expressed in words, codes, schemes or other forms, including amachinereadable medium,capableofcausingacomputertoperform aparticulartaskorachieveaparticularresult.Thewords, codes,schemes, or other formsmaybeprotectedunderCopyrightlaw ascreativeworksthesameas abook, amovie, or aworkofart(andoftentothe coder, the source code is a work of art).

Copyrightprotection extendsfor author'slifetimeplus70years.Forworks madeforhire,theterm ofthecopyrightis 95years fromfirstpublication or 120 years fromcreation, whichever is shorter. Copyright protection is inherent atthetime of creation and is automaticallyprotected, and may appear to be attractive and free option toprotect your software. Additionally, if you wanttobeabletodefinitivelydefinethedateyoucreatedyourcreativework,youcanregisteryourcopyrightwiththeLibraryofCongress.

It should be noted that copyright protects the expression of an idea and not the idea itself. Hence, in thecase of software programs,itisthesoftwareprogramthatisprotected,andnotthefunctionalityofthesoftwareprograms.Unlessyouonlywanttoprotect exactly how the sourcecode is written, it may not be a good idea torely solely on copyright law toprotectsoftwarerelatedinventions.Toprotectthefunctionalityofthesoftwareprogramsyoushouldseekpatentprotection.

PatentProtections

IntheUnitedStatessoftwareispatentable. Softwarepatents aretypicallyreferredtoascomputer implementedprocesses. Software can beprotected intheU.S.ifit is uniqueand tied toamachine.Mostimportantly,forsoftware to be patentable, the software needs tooffer some kind of identifiable improvement. Merelydoing something that is known on acomputer (like addingnumberstogether)isextremelyunlikelytobepatentable.Forexample,U.S.patentlawexcludes"abstractideas",andthishas been used to refuse some patent applications involving software.

InEurope,"computerprogramsassuch"areexcludedfrompatentability.TheEPOholdsthataprogramforacomputerisnotpatentableif itdoes nothavethepotentialtocausea"furthertechnical effect" beyondtheinherenttechnicalinteractionsbetweenhardware andsoftware.

While source codemay not be patentable, it does not mean that a software invention maynot be patented. Oneway of determiningwhetherasoftwareinventionwillbeconsideredpatentablesubjectmatterornot,isbytryingtojudgewhetherthesoftware invention offers atechnicalsolutiontoatechnicalproblem. Theinventionmaybeconsideredpatentablesubject matter if the software invention offers a technical solution to a technical problem.

AdvantagesofPatentsoverCopyrights

Apatentoverasoftwareinventioncanbeusedtopreventothersfromutilizingacertainalgorithmwithoutpermissionortopreventothers from creating software programs that perform patent protected functions.

Incontrast,copyrightlawprotectsonlyaparticularexpressionofanideai.e.copyingofsourcecodeoraportionofit,andnotthecopying of the idea/functionality.

Accordingly,patentsoffermuchbroaderprotection.

Therearesignificantdifferencesintheprotectionsofferedbypatentandcopyright.Hereisasummaryofthedifferencesintheprotections offered by copyrights and patents for software.

Domainnamedisputesincyberspace:

TableofContents

Introduction

Today inthe eraof the internetand technology we gothroughvariouswebsitestolook forsomething.The nameofthepersonisveryimportantfortheiridentityandinthesamewaydomainnameforacompanyis veryimportant.Ifsomeoneusesasimilarorconfusingdomainnameofacompanythenitmightcreateabig problemforacompanyintermsofprofitandgoodwill.Afterreadingthe articleyouwillbe abletounderstand the common issue which generally arises related to the domain name.

Domainname

Adomainnameisliketheaddressorphonenumberofsomeone.Itisacombinationofvarioustypographical characters which are used to describe a location online. Sometimes it is also called a URL(Uniform ResourceLocator). A domain name is very important for any type of business that wants to sell itsproduct online. Two organizationscanneverhavethesamedomainnamesforexamplewww.facebook.com,www.yahoo.com,etc.Inthis example

- WorldWideWeb(www)meansthatthesiteislinkedwiththeworldwideweb.

- .COMis a type of TLD (Top Level Domain). It tells us the service behind the domain name.

The mostcommon Top-leveldomainswhichyouhave seengenerally inthe websitesare (.com,.org,.net) ThesearesomegeneralTLDsthatdon'trequireanywebservicetomeetanyparticularcriteria.Butafter seeingsome TLDsyouwillbeable toknowthe servicetheyprovideforexample (.edu).Itisonly usedfor educationalpurposesonwebsites.SomeTLDsforexample(.us,.in,.fr)arethelocalTLDsthataresupportedto indicate theresourcesoftheparticularcountry.SomeTLDslike(.gov)showthatoperatedbythegovernmentandonly government departments can use such types of domains.

Themaximumlengthis63charactersbutmostarearound2-3.ItcanbespecialaswellasLatincharactersalso.

Typesofdomainnamedisputes

Asknown,acquiringadomainnameforaparticularorganizationisveryimportantifthatorganizationwantstooperate its business online also. Domain name disputes are of various types like cyber squatters, typosquatting, domain name warehousing, cyber twin, reverse domain name hijacking.

Cybersquatting

Cybersquattingcan also be referred to as domain squatting. Cybersquatting is a practice in which a person registersa domain name that resemblesa well-known organization without authorization to gain some profit. Domainregistrantsbuythedomainnamewithamalafide intentionthatharmsthegoodwillandreputationof the company.Thisismainly done togainsome profitby selling the domainname tothe ownerof the original trademarkorservice.Sometimesapersonregistersthenameandexpectsthathewillsellthedomainnamein the future to the highest bid.

Typosquatting

A typosquatterrefers toapersonwhoregistersadomainnamewithcommontyposofthe company'sprimary domain name to shift the traffic from the main website to its website. Let's understand this by taking an exampletosuppose apersonregistersadomainwiththe name www.faceook.comwhichis createdtoshiftthe people from the original site www.facebook.com. This practice is also known as "URL hijacking" or sometimes "web addresshacking."Apersontakesadvantageofcommontypingmistakeswhichpeoplemakewhileenteringany URL.

Cybertwin

Cyber twin refers to when the domain name holder and the person challenging the domain have a legitimate claim to a domain name. In the case before WIPO arbitration and mediation centre name *Indian FarmersFertiliser Cooperation Ltd v. International Foodstuffs Co,(2018)*, the issue was related to the domain name iffco.com.Inthisparticularcase,thedefendantwasusingthedomainnameingoodfaith.Thecomplainant had a legitimateinterestinthedomain,whichwasrelatedtoiffco.com.Thecomplainantstatedthatthedefendantwas diverting the traffic. The arbitration centre dismissed the case and said that both parties had a legitimate interest and the complainant had failed to prove that the defendant was using the domain name in bad faith.

Domainnamewarehousing

Domainnamewarehousingisholdingtheexpireddomaininsteadofreleasingbacktothepublicforbuying.A person containsacertaindomainfrombeingregisteredandhopes toreselltothepreviousownerornewownerata much higher price than the market price. They may try to negotiate to sell at a higher price.

Reversedomainnamehijacking

RDNHstandsforReversedomainnamehijacking(RDNH)isanattemptbythetrademarkholderinbadfaithtotakecontrol of a domain name from another who is having a legitimate interest in the name. According to the Rules15(e)of UniformDomain-Name DisputesResolution Policy(UDRP), it hasbeenstated that whenany complainantisbroughtinbadfaithwhichisprimarytoharassthedomainnameregistrant,thenthepanelcan decide that the complaint is brought in bad faith and constitutes an abuse of administrative proceeding. Reversedomainnamehijackingismostlyenactedbylargecorporationsandindividuals,indefenceoftheir rightful trademark or for preventing libel or slander.

ICANN'SUDRP

Asweallknow,theinternet,whichweknowtoday,beganasthenetworkknownasARPANET(Advanced Research Projects Agency Network, experimental computer network). Internet Assigned Numbers Authority("IANA")managed theinternetby assigning thecomputertotheinternetasanaddress.Somebodies seetherewastheexpansionoftheinternetNetworkSolutions,Inc(NSI),which wastheprivatecompanythat receivedtherighttoassignthedomainaddress.Oneof theICANN'sfirstsubstantiveactswastheadoptionof UDRP, which had three main objectives:

1. Eliminatethejurisdictionandtheproblemoftheconflictinglawrelatedtoallinternetdisputes.
2. Reducethecostofbringingsuitsagainstthecybersquatters.
3. Applyanextremelyrestrictedsetofcircumstancesonlytotheegregiouscases.

AsUDRPincorporatesallregistrationagreementsfor.org,.com,.net.IfanyonewantstofileasuitinUNDP,itis very simple. Firstly the complaint must be filed in one of the alternative dispute resolution bodies which are approvedbytheICANN.Therespondentgetsa20daystimelinetofileareply,afterwhichathree-member committee is formed in which the plaintiff has to prove three elements:

1. Thatthedisputeddomainnameissimilarorconfusing
2. Thattherespondentisnothavinganylegitimateinterestinthedomain
3. Thattherespondentregisteredthedomainnameinbadfaith.

There is a major advantage of using ICANN's UDRP to resolve domain name disputes is that it has a fast preceding.MostofthedecisionsofUDRParehandeddownwithin45daysofthecomplaintbeingfiled.Givingquick decisions is the primary reason for using UDRP.

LegislationgoverningdomainnameinIndia

ThereisnospecificlawrelatedtothedomainnameinIndia,butdomainnamecasesaredecidedundertheTrade Marks Act, 1999.

StarbucksCorporationv.Mohanraj(2009)

This*case*wasrelatedtothedomainnameinwhichdomainwww.Starbucks.co.inwasverysimilartothe complainant www.starbucks.in. Itiscontendedbythecomplainantthattheresponseisnothavinganylegitimateinterest in the domain name and using it in bad faith.

While the respondentsstatedthat at the time of registration the registrar(.in) did not ask for any document to show for registration of trade and also said before the court that the complainant had neglected the domain namedisputeforfouryearsand.co.inwasavailableforusebefore.inextensionwasreleased.Inresponseto the argument given by therespondent, the company stated that the mere fact that at the time of registering thedomainwiththename www.starbucks.co.in the.inregistrydid notask anything didnotbestowuponhim anyabsoluterighttousethesaiddomain.Thecomplainantalsostatedbeforethearbitrator thathehastraded considerably the bonafide right to use the registered trademark Starbucks and the respondent is not having any legitimate interest in the said domain.

Thelearnedarbitrator,afterhearingtheargumentsofboththecomplainantandrespondent,heldthatthe disputed domain name is very similar and confusing to the complainant, and they had the right to the trademark. While answering the question of legitimate interest, it was held by the arbitrator that the respondentdidnotprovideanypositiveandcogentreasontoprovealegitimate interestinthe saiddomain neitherprovidedanyevidenceforsamethereforerespondenthadgotthedomainnameregisteredinbadfaithandheld that domain name to be transferred to the complainant(Starbucks).

GoogleInc.v.GulshanKhatri(2017)

Inthisparticular*case*,acomplaintwasfiledtochallengetheregistrationofthedomainname”googlee.in”.In the complaint, it was stated that the respondent domain name is conceptually, visually identical to the complainant domain name and the respondent tries to ride on the goodwill of the complainant which is built overtheyears.Itwascontendedbythecomplainantthattherespondeddomainname”googlee.in”appeared immediately connected with the complainant. It was also contended that the domain name is used for the searchengineandwouldlikelyperceivethemindofthepublic andgoingtocreateconfusioninthe mindofthe public.Therespondentregisteredthedomainintheyear2007whilethecomplainantdomainname‟google.in”was registered and serving the market way back from the year 1997.

Thearbitratorinthepresentcasestatedthedomainname”googlee.in”wasidenticaltothepriorregistered domainnameanddirectedtheregistrytocancelthesaiddomainnameandtransferthesaiddomaininfavour of the complainant.

AquaMineralsLimitedVs.Mr.PramodBorse&Anr(2001)

Inthisparticular*case*,theHon’bleHighCourtofDelhiruledthatUnlessanduntilapersonishavingacredible explanation as to why he choose a specific name for registering a domain or for that purposeas a trading name that alreadyexistedinthemarketforalongtimeandhadestablisheditsoutstandingreputationandgoodwillthere isno otherinference to be drawn than that the said person wanted to trade in the name of the trade name he had picked up for registration or as a domain name because of its being an incorporated name with huge reputation and goodwill which is achieved at after incurring the huge cost and which is involved in the advertisement of the company.

ElectronicDataBaseanditsProtection:

ImportanceofDataProtectionandPrivacyPoliciesinCyberLaw

TableofContents

Introduction

Thesedaysatermdataprotectionhasbecomesynonymouswithotherrightsofthecitizenswhichareguaranteed by the state. With the beginning of the 21st century, there has been a sharp increase in the development oftechnology, which subsequently has become an integral part of human life. Today, these technologies have connected to the day to day life of a human being in such a way that, these technologies holds important data relatedtoauser.That’swhydataprotectionhasbecomesorelevantinsafeguardingtheinterestofanindividual.

Thisdatarelatedtoanindividualcanalsobecollectedbythewebsites.Wewilllookintotheseconceptsindetail.

Importanceofdataprotectionincyberlaw

WithsteadydevelopmentintheArtificialIntelligence(AI)manysoftwareapplicationslikeFacebook,Googleetc. have developed which not only collect and store the personal data of the user but can also further process the data for any other purpose. In the year 2018, the case of Cambridge Analytica has raised the eyes of many statesover theprotectionofpersonaldataof theircitizens.Thereareabout80 countriesaroundtheworldwho had implemented various privacy policies like GDPR (General Data Protection Regulation) in European Council, Brazil internet Act, 2014 inBrazil, PersonalInformationProtection and ElectronicData Act (PIPEDA) inCanada,etc. to protect their citizen’s personal data.

Thishugenumberofcountriesapparentlyreflectstheconcernsofmanystatesoverthesecurityoftheircitizen’s personal data.Theimplementation ofvarious legislationsaroundthe world,therefore, includesdataprotectionas oneof the branches in cyber law.

DataProtectionunderGeneralDataProtectionRegulations(GDPR)

Inrecenttime,GDPRwasimplementedbytheEuropeanCouncil(EU)in2018andcomesasoneofthestringentlegislation toprotectthepersonaldataofthepeopleoftheEuropeanUnion.Thisregulationhasprovedasa majordevelopmentinthefieldofprivacylaw.Withtheimplementationofthisregulation,therehasbeenamajor impactonthebigtechcompanieslikeGoogle,Facebooketc,andalsoonmanye-commercesites.Thisregulation has certainlysetnewjurisprudenceinthespaceofcyberlaw.WiththeimplementationofGDPR,thewhole domainof privacyrights hasgone to the nextlevel. Let’s discuss someof its features briefly which has put thisregulation far way more ahead with the other regulations around the world.

- **Righttoerasure**[1]–underGDPR,thedatasubjectshavetherighttoerasetheirdata,havingstoredwith any data controller or processor.
- **Rightto dataportability**[2]–underGDPR,thedatasubjectshavetherighttoporttheirpersonal data concerning himself/themselves to one data controller or processor to another.

DataProtectionunderIndianlaw

InIndia,tillnowthereisnoexclusivelawpertainingtotherightsofanindividual’sprivacy.Onlythereis InformationTechnologyact,2000,whichdealswithcybercrimesandprovidesremediesagainsttheviolationof theact.Theactcontainsfewprovisionsrelatedtotheindividual’sprivacybuttheyarenotexhaustiveinnature.

Under**section43AoftheInformationTechnologyAct,2000**[3],abodycorporatewhoispossessing,dealing or handling any sensitive personal data or information of an individual, and is negligent in implementing and maintaining reasonablesecuritypractices inprotecting thedata andresults inwrongfullossor wrongfulgain to anyperson,thensuchbodycorporatemaybeheldliabletopaydamagestothepersonsoaffected.Itisimportant to note that there is no maximum limit specified in the act for the compensation that can be claimed by the affected party in such circumstances.

InformationTechnology(ReasonableSecurityPracticesandProceduresandSensitivePersonalData orInformation)Rules,2011dealswiththeprotectionof‟Sensitivepersonaldataorinformationofaperson”,which includes the personal information relating to:

- Passwords;
- Financialinformationsuchasbankaccountorcreditordebitcardorotherpaymentinstrumentdetails;
- Sexualorientation;
- Medicalrecordsandhistory;and
- Biometricinformation.

Under**section 72A of the Information Technology Act, 2000**[4], disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000.

Under**Section69oftheAct**[5],whichisanexceptiontothegeneralruleofmaintenanceofprivacyandsecrecy of the information, provides that where the Government is satisfied that it is necessary for the interest of:

- thesovereigntyorintegrityofIndia,
- defenceofIndia,
- securityoftheState,
- friendlyrelationswithforeignStates,

- publicorder,
- forpreventingincitementtothecommissionofanycognizableoffencerelatingtoabove,or
- fortheinvestigationofanyoffence.

PenaltyfortheBreachofConfidentialityandPrivacyundertheact

Section72oftheInformationTechnologyact,2000doesn’tspecifytheprovisionrelatingtothebreachofprivacyby thedataprocessorbuttalks aboutacircumstance underwhichany personwho,inpursuanceof any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronicrecord, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person, such person shall be punishable with imprisonment for atermwhich may extend to two years,or with fine which may extendto Rs 1,00,000 or with both.

FuturelegislationrelatedtodataprotectioninIndia

Inthenearfuture,itmightbepossiblethatIndiawillhaveexclusivelegislationrelatedtoProtectionofpersonaldataofan individualinIndia.In2017,thecentralgovernmenthadappointedJusticeBNSrikrishnaCommittee andthiscommitteehadreleasedawhitepaperonDataProtectionlawinIndia.In2018,thecentralgovernment hadpresentedthepersonaldataprotectionbillintheparliamentbutsubsequently,thisbillwasreplacedbythepersonal data protection bill, 2019.

Itisevidentfromthe draftofthe abovementionedbillthat,the billhasbeenformulatedonthe basicprinciples, which were incorporated by the EU General Data Protection Regulations (GDPR). As it becomes necessary to create a balancebetweentherightsofthecitizensand therighttopracticeatradeand economicactivitiesby anentity.

Whatisaprivacypolicy?

Aprivacypolicyisalegaldocumentthatdisclosesthewayapartygathers,uses,discloses,andmanagesa customerorclient’sdata.Itfulfilsalegalrequirementtoprotectacustomerorclient’sprivacy[6].

Suchprivacypolicymustprovidethefollowing[7]:

1. clearlyandeasilyaccessiblestatementsofitspracticesandpolicies;
2. clearlystatethetypeofpersonalandsensitivepersonaldataorinformationcollectedbythebusiness;
3. purposeofcollectionandusageofsuchinformation;
4. aboutdisclosureofinformationincludingsensitivepersonaldataorinformationcollected;and
5. Reasonablesecuritypracticesandproceduresadoptedbyit.

Elementsofaprivacypolicy

Thefollowingarethemainelementswhichshallbeconsistedofaprivacypolicy,areasfollows:

1. **Consent:**Themostcrucialcomponentofaprivacypolicyis‘consent’.Inthisregard,theSupreme CourtinK.S.*Puttuswamy*[8]hasmadeimportantobservations.
2. **Purposeofinformationcollected.**
3. **Disclosureofinformation.**
4. **Securitypractices.**

ITActandCivilProcedureCode:

Fromtheprivacyofyour personaldatastoredwithAadhartoyouronline moviebooking.Fromyourchild’s Instagram posts to yourdematsharetradingaccount. Fromthelegalityofdronesto Uber trackingyour movements…..cyberlaw governsyourentireworld.Youareaffected by cyber law if you use digital technologies – apps, email, social media, smartphones, online banking, onlineshopping,etc.

ThisguidecoversIndiancyberlaw.Ifyouarelookingforglobalcyberlaws,seeTheUltimateGuidetoGlobalCyberLaws.
Theprimary sourceofcyberlaw inIndiaisthe **InformationTechnologyAct,2000** (ITAct)thatcameintoforceon17thOctober2000. Thecyber lawecosysteminIndiaconsistsoftheITAct(asamendedfromtimetotime)anditsalliedActs,Orders,Guidelines,Regulations, and Rules.
InIndia,cyber lawsare primarilyunder thegovernance ofthe MinistryofElectronics&InformationTechnology,GovernmentofIndia.The**IndianPenalCode**(asamendedbytheInformationTechnologyAct)penalizesseveralcybercrimes.Theseincludeforgeryofelectronic records, cyber frauds, destroying electronic evidence, etc.
DigitalEvidenceistobecollectedandprovenincourtaspertheprovisionsofthe**IndianEvidenceAct**(asamendedbytheInformationTechnologyAct).
Inthecaseofbankrecords,theprovisionsofthe**Bankers’BookEvidenceAct**(asamendedbytheInformationTechnologyAct)arerelevant.Investigationan adjudicationofcybercrimesisdoneinaccordancewiththeprovisionsofthe **CodeofCriminalProcedure**,**CivilProcedure Code,** and the **Information Technology Act**.TheInformationTechnologyActalsoamendedthe **ReserveBankofIndiaAct**pavingthewayfordigitalpayments.

DiplomainCyberLaw
LookingtobuildyourexpertiseinthecyberlawsofIndia?ChecktheoutDiplomainCyberLawconductedbyASCLjointlywithGovernment Law College Mumbai.

TableofContents

1. TheNeedforCyberLaw

Isthereaneedforaseparatefieldoflawtocovercyberspace?Isn’tconventionallawadequatetocovercyberspace?

Letusconsidercaseswhereso-called**conventionalcrimesarecarriedoutusingcomputers**ortheInternetasatool.Considercasesof spread of pornographic material, criminal threats delivered via email, websites that defame someone or spreadracialhatred,etc. Inallthesecases, thecomputerismerelyincidentaltothecrime.Distributingpamphlets promotingracialenmityisinessence similar to putting up a website promoting such ill feelings.
Of course, it can be argued that when technology is used to commit such crimes, the effect and spread of the crimeincreasesenormously.Printinganddistributingpamphletseveninonelocalityisatimeconsumingandexpensivetaskwhileputtingupa globally accessible website is very easy.

Insuchcases,itcanbearguedthatconventionallawcanhandlecybercases. TheGovernmentcansimply imposea stricter liability(by wayofimprisonmentandfines) ifthecrime iscommittedusingcertain specified technologies.A simplifiedexamplewouldbestatingthatspreadingpornographybyelectronic meansshouldbepunishedmoreseverelythanspreadingpornographybyconventionalmeans.

Aslongaswearedealingwithsuchissues, conventional lawwouldbeadequate.Thechallengesemergewhenwedealwithmorecomplexissuessuchas**‘theft’ofdata**.
Underconventionallaw,theftrelates to “movablepropertybeingtakenoutof thepossessionofsomeone”.

TheGeneralClausesActdefines**movableproperty**as“propertyofeverydescription,exceptimmovableproperty”.Thesamelawdefines**immovableproperty** as“land,benefitstoariseoutofland, andthings attachedtotheearth,orpermanentlyfastenedtoanythingattached to the earth”. Using these definitions, we can say that the computer is movable property.

Let us examine how such a law wouldapply to a scenario where **data is ‘stolen’.** Consider my personal computer on which Ihavestored some information. Let us presume that some unauthorized person picks up my computer and takes it away withoutmypermission. Has he committedtheft? The elements to consider are whether some movable property has been taken out ofthepossessionofsomeone.ThecomputerismovablepropertyandIamthelegalownerentitledtopossessit.Thethiefhasdishonestlytakent his movable property out of my possession. It is theft.

Now consider that some unauthorized person simply **copies the data** from my computer onto his pen drive. Would this betheft?Presumingthattheintangibledataismovableproperty,theconceptoftheftwouldstill notapply asthepossessionofthedatahasnotbeentakenfrom me.Istillhavethe‘original’dataonthecomputer undermycontrol.The ‘thief’simplyhasa‘copy’ofthat data.In thedigital world, the copy and the original are indistinguishable in almost every case.

Consider another illustration on the issue of **‘possession’** of data. I use the email account rohasnagpal@gmail.com forpersonalcommunication. Naturally, alotof emails, images, documents etc aresent andreceivedby me usingthis account. Thefirstquestionis,who‘possesses’thisemailaccount?IsitmebecauseIhavetheusernameandpasswordneededto‘login’andviewtheemails?Oritis Google Inc because the emails are stored on their computers?

Anotherquestionwouldariseifsomeunauthorizedpersonobtainsmypassword.Canitbesaidthatnowthatpersonisalsoinpossessionof my emails because he has the password to ‘login’ and view the emails?

Another legal challenge emerges because of the **‘mobility’** of data. Let us consider an example of international trade intheconventionalworld.SameerpurchasessteelfromafactoryinChinausesthesteeltomanufacturenailsinafactoryinIndiaandthensellsthe nails to a trader in the USA. The various Governments can easily regulate and impose taxes at various stages ofthisbusinessprocess.

Now consider that Sameer has shifted to an ‘online’ business. He sits in his house in Pune (India) and uses his computer tocreatepiratedversionsofexpensive software. He thensellsthis piratedsoftwarethrougha website(hostedonaserver locatedinRussia).PeoplefromallovertheworldcanvisitSameer’swebsiteandpurchasethepiratedsoftware. Sameercollectsthemoneyusing aPayPal account that is linked to his bank account in a tax haven country like the Cayman Islands.

ItwouldbeextremelydifficultforanyGovernmenttotraceSameer’sactivities.

Itisfortheseandothercomplexitiesthatconventionallawisunfittohandleissuesrelatingtocyberspace.Thisbringsintheneedforaseparate branch of law to tackle cyberspace.

2. Whatdoescyberlawcover?

CyberLawisthelegalandregulatoryframeworkrelatingto

1. ArtificialIntelligence
2. Bitcoin&othercrypto-currencies
3. Cloudcomputing
4. CryptographyExport
5. CyberCrimeInvestigationandForensics
6. CyberInsurance
7. Cybersecurityandincidentresponse
8. CyberTerrorism&Warfare
9. Databreachesanddataprivacy
10. DigitalEvidence
11. Digitalpayments,credit,debit&cashcards,mobilewallets,netbanking,UPI
12. Domainnamedisputes
13. E-commerce
14. E-governance,E-courts&E-tenders
15. Electronic&DigitalSignatures
16. Electroniccontracts
17. Electronicvotingmachines
18. Extraditionofcybercriminals
19. Hacking,malware,ransomware,andothercybercrimes,
20. InformationTechnologyLawCompliance
21. IntermediarieslikeInternetServiceProviders(ISPs),SocialMediaPlatforms,Emailservices,videostreamingservices

22. InternetofThings
23. Onlineeducation
24. Onlinegambling&gaming,andpharmacies
25. Onlinesharetrading,banking,andtaxfiling
26. Softwarelicenses
27. Spam,hatespeechandtrolling
28. Telemedicine
29. Torrents,darkweb,p2pnetworks,andfile-sharing
30. Videoconferencing

3. InformationTechnologyAct

ThemajorissuesaddressedbytheITActrelateto:

1. electronicrecords
2. establishingofauthorities
3. CertifyingAuthorities
4. cybercrimes
5. administrativeissues
6. amendments

TheInformationTechnologyActdoesnotapplyto:

1. anegotiableinstrument(otherthanacheque),
2. apower-of-attorney,
3. atrust,
4. awill
5. anycontractforthesaleorconveyanceofimmovablepropertyoranyinterestinsuchproperty
6. anysuchclassofdocumentsortransactionsasmaybenotifiedbytheCentralGovernmentintheOfficialGazette.Cybercrimesunder

Chapter9oftheITActcomeunderthejurisdictionof**AdjudicatingOfficers**.AppealsfromordersoftheAdjudicatingOfficers lie tothe**CyberAppellateTribunal** andappealsfromtheordersof the CyberAppellateTribunallietothe **HighCourt**.Othercybercrimes come under the jurisdiction of the **criminal courts**.
Case law is the law that is established through the decisions of the courts and other officials. Case law assumes evengreatersignificancewhenthewordingsofaparticularlawareambiguous.TheinterpretationoftheCourtshelpsclarifytherealobjectivesandmeaning of such laws.
InIndia,courtsareboundbydecisionsofhighercourtsinthehierarchy.TheapexcourtinIndiaisthe**SupremeCourt**.Article141oftheConstitution ofIndia statesthat “the lawdeclaredbythe Supreme Courtshallbe bindingon allcourts within the territoryofIndia”.
The hierarchy of courts is further enshrined in the **Code of Civil Procedure, 1908** and the **Code of Criminal Procedure,1973**.ThechiefresponsibilityofAdjudicatingOfficers(AO)undertheITActistoadjudicateoncasesundersection43,44and45oftheITActe.g.unauthorizedaccess, unauthorizedcopyingof data,spreadof viruses, denialof serviceattacks,computermanipulations etc.

CertifyingAuthorities,the**Controller**andotherofficers/agenciesestablishedundertheActandothergovernmentagencieslikeCERT-IND are required to promptly assist the AO.
AppealsagainsttheordersofAOandtheControllerliewiththe**CyberAppellateTribunal**.TheprimaryroleoftheControllerofCertifyingAuthorities(CCA)istoregulatetheworkingofthe **CertifyingAuthorities**(CA).ACA is abusinessorganizationthatissuesdigitalsignaturecertificatestosubscribers.Thissetsthebaseforthedevelopmentofelectroniccommerce and governance in India.
TheCCAalsohasinvestigationpowersu/s28oftheITAct.TheCCAcanalsodirectapersontodecryptinformationunderhiscontrol.Ifsucha person refuses to comply with the CCA directions he faces 7 years imprisonment u/s 69 of the IT Act.

Theinvestigationofcybercrimescoveredbythe **IndianPenal Code** isdonebythe **police**.ForcybercrimescoveredbytheITAct,investigation can be done by an officer not below the rank of a Inspector of police.Accordingtosection2(h)oftheCodeofCriminalProcedure,“investigation”includesall theproceedingsunderthisCodeforthecollectionofevidenceconductedbya policeofficerorbyany person(otherthanaMagistrate)whoisauthorisedbyaMagistrateinthisregard.

Section28oftheInformationTechnologyActempowersthefollowingtoinvestigateanycontraventionoftheActandalliedrulesandregulations: (1) the Controller (2) any officer authorised by the Controller.

Additionally,section78oftheInformationTechnologyActempowersapoliceofficernotbelowtherankofInspectortoinvestigateoffenceunder the Act. Offences are defined under Chapter XI of the Act.

Additionally,rule4(i)ofthe **InformationTechnology(QualificationandExperienceofAdjudicatingOfficersandMannerofHolding Enquiry) Rules, 2003** authorizes the Adjudicating Officer to get a matter orreportinvestigatedfromanofficerintheOfficeofControllerorCERT-INDorfromtheconcernedDeputy Superintendent ofPolice[Inspector], to ascertainmore facts andwhether prima facie there is a case for adjudicating on the matter ornot.
Additionally, section 80 of the Information Technology Act provides a special power to police officers not below the rank ofanInspectorofPoliceandtootherGovernmentofficersauthorisedbytheCentralGovernment.Suchauthorisedpersonscanenterandsearchany public place. Public places include cyber cafes, hotels, shops etc accessible to the public.

Additionally,theycanarrestwithoutwarrantanypersonfoundinsuchapublicplacewhoisreasonablysuspectedof:

1. havingcommittedanoffenceundertheAct,
2. committinganoffenceundertheAct,
3. beingabouttocommitanyoffenceundertheAct.

4. ChronologyoftheIndianCyberLaw20
00

The primarysourceofcyber lawinIndiaisthe **InformationTechnologyAct,2000**(ITAct)whichcameinto forceon17thOctober2000.The primary purpose of the Information Technology Act is to provide legal recognition to electronic commerce and tofacilitatefilingofelectronicrecordswiththeGovernment.TheInformationTechnologyActalsopenalizesvariouscybercrimesandprovidesstrictpunishments (imprisonment terms up to 10 years and compensation up to crores of rupees).
The**IndianPenalCode**(asamendedbytheInformationTechnologyAct)penalizesseveralcybercrimes.Theseincludeforgeryofelectronic records, cyber frauds, destroying electronic evidence etc.
DigitalEvidenceistobecollectedandproveninсourtaspertheprovisionsoftheIndianEvidenceAct(asamendedbytheInformationTechnologyAct).
Incaseofbankrecords,theprovisionsofthe**Bankers'BookEvidenceAct**(asamendedbytheInformationTechnologyAct)arerelevant.Investigationandadjudicationofcybercrimesisdoneinaccordancewiththeprovisionsofthe**CodeofCriminalProcedure**,**CivilProcedure Code** and the **Information Technology Act.**
The**ReserveBankofIndiaAct**wasalsoamendedbytheInformationTechnologyAct.
On 17th October 2000, the **Information Technology (Certifying Authorities) Rules, 2000** also came into force. Theserulesprescribetheeligibility,appointmentandworkingofCertifyingAuthorities.Theserulesalsolaydownthetechnicalstandards,procedures and security methods to be used by a Certifying Authority.
The **Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000** also came into force on 17th October 2000. TheserulesprescribetheappointmentandworkingoftheCyberRegulationsAppellateTribunalwhoseprimaryroleistohearappealsagainst orders of the Adjudicating Officers.

2001

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9th July 2001. They providefurthertechnicalstandardsandprocedurestobeusedbyaCertifyingAuthority.TwoimportantguidelinesrelatingtoCertifyingAuthoritieswere issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority undertheInformation Technology Act. These guidelines were issued on 9th July 2001.

2002

An**ExecutiveOrder**dated12thSeptember2002containedinstructionsrelatingprovisionsoftheActwithregardtoprotectedsystemsand application for the issue of a Digital Signature Certificate.
Nextwerethe **GuidelinesforsubmissionofcertificatesandcertificationrevocationliststotheControllerofCertifyingAuthoritiesfor publishing in National Repository of Digital Certificates**. These were issued on 16th December 2002.
MinorerrorsintheActwererectifiedbythe**InformationTechnology(RemovalofDifficulties)Order,2002**whichwaspassedon19thSeptember 2002.
TheInformationTechnologyActwasamendedbythe**NegotiableInstruments(AmendmentsandMiscellaneousProvisions)Act, 2002**. This introduced the concept of electronic cheques and truncated cheques.
Cyber Regulations Appellate Tribunal (Salaries, Allowances and Condition of Service of other Officers andEmployees)Rules,2002werepassed.ThisprovidesforthenatureandcategoriesofofficersandemployeesoftheCyberAppellateTribunalandtheir scales of pay. Further, the Rules also provide for the regulation of the conditions of service of officers andemployees of theCyber Appellate Tribunal in the matter of pay, allowances, leave, joining time, provident fund, age ofsuperannuation, pension andretirement benefits, medical facilities, conduct, disciplinary matters and other conditions.

2003

On 17th March 2003, the **Information Technology (Qualification and Experience of Adjudicating Officers and MannerofHoldingEnquiry)Rules,2003**werepassed.TheserulesprescribethequalificationsrequiredforAdjudicatingOfficers.Theirchiefresponsibility under theIT Actis to adjudicate casessuchasunauthorized access, unauthorizedcopying ofdata, spreadofviruses,denialofserviceattacks,disruptionofcomputers,computer manipulationetc.Theserulesalsoprescribethemanner andmodeofinquiryandadjudication by these officers.
The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the**PublicInterest Litigation (PIL) filed by students of Asian School of Cyber Laws** (ASCL). The Government had notappointedAdjudicatingOfficersortheCyberRegulationsAppellateTribunalfor almost 2yearsafter the passageofthe IT Act.ThispromptedASCLstudentstofilea PublicInterest Litigation(PIL)intheBombayHighCourt askingfor aspeedyappointmentofAdjudicatingofficers.
TheBombayHighCourt,initsorder dated9thOctober2002,directedtheCentral Governmentto announcetheappointmentofadjudicatingofficersinthe publicmediatomake peopleawareoftheappointments.The divisionbenchoftheMumbai HighCourt

consistingofHon’bleJusticeA.P.ShahandHon’bleJusticeRanjanaDesaialsoorderedthattheCyberRegulationsAppellateTribunalbeconstitutedwithinareasonabletimeframe.

Followingthis,the**Central Governmentpassedanorderdated23rdMarch2003**appointingthe“SecretaryofDepartmentofInformationTechnologyofeachofthe States or of Union Territories” of India as the adjudicating officers.
The **Cyber Regulations Appellate Tribunal (Salary, Allowances and other Terms and Conditions of Service ofPresidingOfficer)Rules,2003**prescribethesalary,allowances andother termsforthePresidingOfficeroftheCyberRegulationsAppellateTribunal.**InformationTechnology(OtherPowersofCivilCourtVestedinCyberAppellateTribunal)Rules 2003** providedsome additional powers to the Cyber Regulations Appellate Tribunal.
Also relevant are the **Information Technology (Other Standards) Rules, 2003**. An important order relating to blockingofwebsites was passed on 27th February, 2003. Under this, Computer Emergency Response Team (CERT-IND) caninstructDepartmentofTelecommunications(DOT)toblockawebsite.The**InformationTechnology(CertifyingAuthorities)Rules,2000**wereamended.The**ChhattisgarhCitizenService(ElectronicGovernance) Rules, 2003** were passed for effectiveimplementation of e-governance services.

2004

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 have provided the necessarylegalframeworkforfilingofdocumentswiththeGovernmentaswellasissueoflicensesbytheGovernment.Italsoprovidesforpaymentandreceipt of fees in relation to Government bodies.
The**InformationTechnology(SecurityProcedure)Rules,2004**cameintoforceon29thOctober2004.Theyprescribeprovisionsrelating to secure digital signatures and secure electronic records.
The**InformationTechnology(CertifyingAuthorities)Rules,2000**wereamended.
The**GujaratInformationTechnologyRules,2004**werepassedinordertoregulatecybercafesintheStateofGujarat.TheRulesprovidefor maintenance of log register by cyber cafe owners, the responsibilities of cyber cafe owners, etc.
The **InformationTechnology(Karnataka) Rules,2004**were issued inordertoregulatecybercafesinthe State ofKarnataka.TheRulesprovideformaintenanceoflogregister bycybercafeowners,theresponsibilities ofcybercafeowners, liabilityincaseofnon-compliance,etc.

2006

The**InformationTechnology(CertifyingAuthorities)Rules,2000**wereamended.

2007

The**RajasthanCyberCafeRules,2007**werepassedwithaviewtoregulatecybercafesinRajasthan.TheRulesprovideformaintenance oflogregister bycybercafeowners,theresponsibilitiesofcybercafeowners,etc.

2009

The**InformationTechnology(Amendment)Act,2008**,whichcameintoforceon27thOctober,2009hasmadesweepingchangestothe Information Technology Act.Thefollowingruleshavealsocomeintoforceon27thOctober,2009:

1. **InformationTechnology(ProcedureandSafeguardsforInterception,MonitoringandDecryptionofInformation)Rules,2009.**
2. **InformationTechnology(ProcedureandSafeguardforMonitoringandCollectingTrafficDataorInformation)Rules,2009.**
3. **InformationTechnology(ProcedureandSafeguardsforBlockingforAccessofInformationbyPublic)Rules,2009.**
4. **TheCyberAppellateTribunal(Salary,AllowancesandOtherTermsandConditionsofServiceofChairpersonand Members)Rules,2009.**
5. **CyberAppellateTribunal(ProcedureforInvestigationofMisbehaviourorIncapacityofChairpersonandMembers)Rules,2009.**

The**InformationTechnology(CertifyingAuthorities)Rules,2000**wereamended.

2010

The**KeralaInformationTechnology(ElectronicDeliveryofServices)Rules,2010**passedtoimprovedeliveryofe-servicesbytheGovernment.

2011

InformationTechnology(Reasonablesecuritypracticesandproceduresandsensitivepersonaldataorinformation)Rules,2011 passed.Theserulesdefinesensitivepersonaldataorinformationandformthecruxofndia’sdataprivacylaw.Clarificationon**InformationTechnology(Reasonablesecuritypracticesandproceduresandsensitivepersonaldataorinformation) Rules, 2011** were also issued.
InformationTechnology(Intermediariesguidelines)Rules,2011passed.Theserulesexplaintheduediligencetobeobservedbyintermediaries.
InformationTechnology(ElectronicServiceDelivery)Rules,2011passed.TheserulesrelatetothesystemofElectronicServiceDelivery by the Government.**InformationTechnology(GuidelinesforCyberCafe)Rules,2011**passed.Thisprovidesforregistrationofcybercafes,maintenanceoflog register, identification of user, etc.
The**AndhraPradeshInformationTechnology(ElectronicServiceDelivery)Rules,2011**wereissuedtoimprovedeliveryofe-servicesby the Government.
The **Madhya Pradesh Information Technology (Regulation of Electronic Delivery of Citizen Services and AppointmentofServiceProvider)Rules,2011**werepassedtoregulatetheelectronicdeliveryofcitizenservices,appointmentofserviceproviderandforthe purpose of effective implementation of e-governance services.

2013

Clarification on **The InformationTechnology (Intermediary Guidelines)Rules,2011** issued.According to it,intermediariesshouldhaveapubliclyaccessibleandpublishedgrievanceredressalprocessbywhichcomplaintscanbelodged.Italsoclarifiesthewords “..shall act within thirty-six hours.” as mentioned in sub-rule (4) of Rule 3.
Information Technology (National Critical Information Infrastructure Protection Centre and Manner ofPerformingFunctionsandDuties)Rules,2013cameintoforce.TheylaydownthefunctionsanddutiesoftheNationalCriticalInformationInfrastructure Protection Centre.**Information Technology (The Indian Computer Emergency Response Team and Manner of Performing FunctionsandDuties)Rules,2013**cameintoforce.Theylaydownthedetailedfunctions,responsibilitiesandservicesoftheIndianComputerEmergency Response Team.

InformationTechnology(Salary,AllowancesandTermsandConditionsofServiceoftheDirectorGeneral,IndianComputerEmergency Response Team) Rules, 2012 were passed on 24th January 2013 regulating the qualifications, experience and othertermsand conditions of service of the Director General, Indian Computer Emergency Response Team.
Information Technology (Recognition of Foreign Certifying Authorities Operating under a RegulatoryAuthority)Regulations,2013cameintoforceinordertoregulatetheconductofForeignCertifyingAuthoritiesinIndiaoperatingunderaregulatoryauthority.
Information Technology (Recognition of Foreign Certifying Authorities not Operating under a RegulatoryAuthority)Regulations,2013cameintoforceinordertoregulatetheconductofForeignCertifyingAuthoritiesinIndianotoperatingunderaregulatoryauthority.

2015

UniqueIdentificationAuthorityofIndia(UIDAI)facilities,InformationAssets,LogisticsInfrastructureandDependenciesdeclaredasprotected systems under section 70 of the Information Technology Act.

DigitalSignature(EndEntity)Rules,2015cameintoforce.Theydealwithlongtermvaliddigitalsignatures.**InformationTechnology(SecurityProcedure)AmendmentsRules,2015**cameintoforce.TheymakeminoramendmentstotheInformationTechnology(SecurityProcedure) Rules, 2004.
InformationTechnology(CertifyingAuthorities)AmendmentRules,2015cameintoforce.TheymakeamendmentstoInformationTechnology (Certifying Authorities) Rules, 2000.

2016

IndianComputerEmergencyResponseTeamauthorisedtomonitorandcollecttrafficdataorinformationgenerated,transmitted,receivedorstoredinanycomputerresource.ElectronicSignatureorElectronicAuthenticationTechniqueandProcedureRules,2016passed.Theselaydownthemannerinwhichtheinformation is authenticated by means of digital signatures.

InformationTechnology(CertifyingAuthorities)(Amendment)Rules,2016passed.TheserulesmadeaslightcorrectiontotheInformation Technology (Certifying Authorities) Rules, 2000.
CyberAppellateTribunal(PowersandFunctionsoftheChairperson)Rules,2016passed.Theseruleslaydownthepowersandfunctions of the Chairperson of the Cyber Appellate Tribunal.
Advisory on Functioning of Matrimonial Websites in accordance with the Information Technology Act, 2000 and Rulesissued.Accordingtothisadvisory, "Therehavebeeninstanceswhereusersofmatrimonialwebsites falsifytheirmaritalstatus,age,height,personality,health, socialandeconomicstatus.Inmostofthecasesvictimsarewomenwhofall preytothesefraudstersaftergetting introduced through fake profiles on matrimonial portal". This advisory has been issued to strengthen protectivemeasuresfor all users of such websites.
Aadhar(TargetedDelivery ofFinancial andotherSubsidies,BenefitsandServices)Act,2016cameintoforceon26thMarch2016.Throughthislegislation,thegovernmentplanstotargetdeliveryofsubsidiesandservicesby assigninguniqueidentitynumberstoindividuals residing in India.
InformationTechnology(PreservationandRetentionofInformationbyIntermediariesProvidingDigitalLockerFacilities)Rules,2016 were passed for the preservation and retention of information by intermediaries providing Digital Locker Facilities.

2017

TheGovernmentOpenDataLicenseNationalDataSharingandAccessibilityPolicywasannouncedon10thFebruary,2017.

2018

On22ndMay,2018,the**InformationTechnology(InformationSecurityPracticesandProceduresforProtectedSystem)Rules,2018** came into force. These rules prescribe information security practices and procedures for protected systems.
On 20th December, 2018, the following Security and Intelligence Agencies were authorised for the purposes ofinterception,monitoringanddecryptionofanyinformationgenerated,transmitted,receivedorstoredinanycomputerresourceundertheInformation Technology Act:

1. IntelligenceBureau;
2. NarcoticsControlBureau;
3. EnforcementDirectorate;
4. CentralBoardofDirectTaxes;
5. DirectorateofRevenueIntelligence;
6. CentralBureauofInvestigation;
7. NationalInvestigationAgency;
8. CabinetSecretariat(RAW);
9. DirectorateofSignalIntelligence(ForserviceareasofJammu&Kashmir,North-EastandAssamonly);
10. CommissionerofPolice,Delhi.

2019

TheCentralGovernmentnotifiedtheRegionalForensicScienceLaboratory,NorthernRange,Dharamshala,District-Kangra(HimanchalPradesh), as Examiner of Electronic Evidence within India, with the following scope:

1. Computer(Media)ForensicsexcludingFloppyDiskDrive;
2. MobileDevicesForensics.

ITActandCriminalProceduralCode:

Defining"CyberCrimes"
Theterm"cyber-crimes"isnotdefinedinanystatuteorrulebook.Theword"cyber"isslangforanythingrelatingtocomputers, information technology, internet and virtual reality. Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, internet and virtual reality.

One finds lawsthat penalisecyber-crimesina number ofstatutes and even in regulationsframed byvarious regulators.The InformationTechnologyAct, 2000("ITAct")andtheIndianPenal Code, 1860("IPC")penaliseanumberofcyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other.

ParallelProvisionsintheIPCandITAct
Manyofthecyber-crimes penalisedbytheIPCandtheITActhavethesameingredients andevennomenclature.Herearea fewexamples:

Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computernetwork,datatheft,introducing andspreadingvirusesthroughcomputernetworks,damagingcomputersorcomputer networks orcomputerprogrammes,disruptinganycomputerorcomputersystemorcomputernetwork,denyinganauthorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or afineor Rs. 5,00,000 (Rupees five lac) or both.

Section 378 of theIPC relating to"theft" of movableproperty will applytothetheft of anydata, onlineor otherwise, since section22oftheIPCstatesthatthewords"movableproperty" areintendedtoincludecorporealpropertyof everydescription, except landandthings attachedtotheearthorpermanentlyfastenedtoanythingwhichis attachedtotheearth.Themaximum punishment for theft under section 378 of theIPC is imprisonment of up to3(three) years or afine or both.

Itmaybearguedthattheword"corporeal" whichmeans'physical'or'material'wouldexcludedigital propertiesfrom theambit of theaforesaidsection378oftheIPC.Thecounterargument wouldbethatthedraftersintendedtocoverproperties ofevery description, except land and things attached to the earth or permanentlyfastened toanything which is attached to the earth.

Section 424 of the IPC states that "*whoever dishonestly or fraudulently conceals or removes any property of himself or any otherperson,ordishonestlyorfraudulentlyassistsintheconcealmentorremovalthereof, ordishonestlyreleasesanydemand or claim towhichheis entitled,shallbepunishedwithimprisonmentofeither description*[1]*for atermwhichmayextendto2(two)years, or with fine, or with both.*" This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or afine or both.

Section425oftheIPCdeals withmischiefandstatesthat "*whoeverwithintenttocause, orknowingthat heislikelytocause, wrongful lossordamagetothepublic ortoany person,causes thedestructionofany property,oranysuchchangeinanypropertyor in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief*".
Needless to say, damaging computer systems and even denying access to a computer system will fall within theaforesaid section425oftheIPC.Themaximumpunishmentformischiefaspersection426oftheIPCisimprisonmentofupto3(three)monthsor a fine or both.

Receipt of stolen property: Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestlyorshouldhavereasontobelievethatitwasstolenproperty.ThepunishmentforthisoffenceunderSection66BoftheITActis imprisonment of up to 3 (three) years or afine of up to Rs. 1,00,000 (Rupees one lac) or both.

Section 411 of theIPC too prescribes punishment for dishonestlyreceivingstolen property andisworded in a manner that is almostidenticaltosection66BoftheITAct.Thepunishmentundersection411oftheIPCisimprisonmentofeitherdescriptionforaterm ofup to3 (three)years,or with fine, or with both. Please note that the only differencein the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

Identitytheft and cheatingbypersonation: Section66C of theITActprescribes punishment foridentitytheft andprovides thatanyonewhofraudulentlyordishonestlymakesuseoftheelectronicsignature,passwordoranyotheruniqueidentificationfeature ofanyotherpersonshallbepunishedwithimprisonmentof eitherdescriptionforaterm whichmayextendto3(three)years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 66D of theITActprescribes punishmentfor'cheating by personation byusingcomputerresource' andprovides that anypersonwhobymeans of anycommunicationdeviceorcomputerresourcecheats bypersonation,shallbepunishedwith imprisonmentof either descriptionfor atermwhich mayextendto3(three) years andshallalsobeliabletofinewhichmay extend to Rs. 1,00,000 (Rupees one lac).

Section419of theIPC alsoprescribes punishmentfor'cheatingbypersonation'andprovides thatanypersonwhocheats by personationshallbepunishedwithimprisonmentof eitherdescriptionforatermwhichmayextendto3(three)years orwitha fineorwithboth.A personissaidtobeguiltyof'cheatingbypersonation' ifsuchpersoncheatsbypretendingtobesomeother person, or byknowinglysubstituting onepersonfor another, orrepresentingthat he or any otherpersonis a personotherthan he orsuch other person really is.

Theprovisionsofsections463, 465and468oftheIPCdealingwithforgeryand"forgeryforthepurposeofcheating",mayalso be applicablein acase of identitytheft. Section 468 of theIPC prescribes punishmentfor forgeryforthepurpose of cheatingand provides a punishment of imprisonment of either descriptionfor aterm which may extendto 7(seven) years and alsoafine. Forgery has been definedinsection463 of theIPCtomeanthemaking of afalsedocument or partthereof with theintenttocause damageor injury,tothepublic or toanyperson,ortosupportanyclaimor title, or tocauseanypersontopart withproperty,or to enter into any express or implied contract, or with intent tocommit fraud or that fraud may be committed.

Inthiscontext, referencemayalsobemadetosection420oftheIPCthatprovidesthat anypersonwhocheats andthereby dishonestlyinducesthepersondeceivedtodeliveranypropertytoanyperson,ortomake,alterordestroy thewholeorany part of a valuablesecurity, or anythingwhichissignedorsealed,and whichiscapableof beingconvertedintoavaluablesecurityshall bepunishedwithimprisonmentofeitherdescriptionforaterm whichmayextendto7(seven)years, andshall also be liable to fine.

Theonlydifferencebetweenthepunishmentsprescribedundersections66Cand66DoftheITActandsection419oftheIPCisthatthere is nomaximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that theimprisonment mat extend to 7 (seven) years. Further, whilst theITAct contemplatesboth theimposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offencecould be punished with imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation tothe offenceof identitytheft is that the latter requires the offence to be committed with the help of a computer resource.

Obscenity:Sections67,67A and67BoftheITActprescribepunishmentforpublishingortransmitting,in electronicform:(i) obscenematerial;(ii)materialcontainingsexuallyexplicitact,etc.; and(iii)materialdepictingchildreninsexually explicitact, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on thefirst conviction, imprisonment of either description for aterm which may extend to3 (three) years, to beaccompanied bya fine which may extend toRs. 5,00,000 (Rupees five lac), and in the event of asecond or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by afine which may extend toRs. 10,00,000 (Rupees ten lac). The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of eitherdescriptionforaterm whichmayextendto5(five)years,tobeaccompaniedbyafinewhichmayextend to Rs. 10,00,000 (Rupeestenlac)and in theevent ofsecond orsubsequent conviction, imprisonment of either descriptionfor a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lac).

Theprovisionsofsections292and294oftheIPCwould alsobeapplicableforoffences ofthenaturedescribedundersections 67, 67A and67B of theIT Act. Section 292 of theIPC provides that any person who, inter alia,sells, distributes, publicly exhibitsor in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representationorfigureor anyother obsceneobject whatsoevershallbepunishableonafirstconviction withimprisonment of either description for a term which may extend to 2 (two) years, andwith finewhich may extend to Rs. 2,000 (Rupees two thousand)and,intheeventofasecondorsubsequentconviction,withimprisonmentofeitherdescriptionforatermwhichmayextendto5 (five) years, to be accompanied by afine which may extend to Rs. 5,000 (Rupees five thousand).

Section294oftheIPCprovidesthatanypersonwho,totheannoyanceofothers,does anyobsceneactinanypublicplace,or sings, recites orutters anyobscenesong,ballad orwords,inornearanypublicplace,shallbepunished withimprisonment of eitherdescription for a term which may extend to 3 (three) months, or with fine, or with both.

Cyber-crimesnotprovidedforintheIPC
Thefollowingcyber-crimespenalisedbytheITActdonothaveanequivalentintheIPC.

Section43(h)oftheITAct:Section43(h)readwithsection66oftheITActpenalisesanindividualwhochargestheservices availedofbyapersontotheaccountofanotherpersonbytamperingwithormanipulatinganycomputer,computersystem, or computernetwork.Apersonwhotamperswiththecomputersystemofanelectricitysupplierandcauseshisneighbourtopayforhis electricityconsumptionwouldfallundertheaforesaidsection43(h) of theITActfor whichthereis noequivalentprovisionin theIPC.

Section65 ofthe IT Act: Section65 of the ITAct prescribes punishment for tampering withcomputersource documents and provides that any person who knowingly or intentionallyconceals, destroys or alters or intentionally or knowinglycauses anothertoconceal,destroy,oralteranycomputersourcecode(i.e.alistingofprogrammes,computercommands,designandlayoutand programme analysis of computer resource in any form) used for a computer, computer programme, computer system orcomputer network, when thecomputer sourcecode is required to bekept ormaintained bylawfor the time beingin force,shall bepunishablewithimprisonmentforupto3(three)yearsorwithafinewhichmayextendtoRs.3,00,000(Rupees lac) or with both.

Toacertain extent, section 409 of theIPC overlaps withsection 65 of theITAct. Section 409 of theIPC provides that any personwhois inanymannerentrustedwithproperty,orwithanydominionoverpropertyinhiscapacityas apublicservant or inthewayofhis businessasabanker,merchant,factor,broker,attorneyoragent,commitscriminalbreachoftrustinrespect of that property, shall be punished with imprisonment for lifeor with imprisonment ofeither description foraterm which may extend to10 (ten) years, and shall alsobe liable to a fine. However, section 65 of the IT Act does not requirethat the person who tampers withor damages or destroys computer sourcedocumentsshouldhavebeen entrustedwithsuchsourcecode. Under section409oftheIPC,criminalbreachoftrustshouldhavebeencommittedbysomeonetowhomthepropertywas entrusted.

Violationofprivacy:Section66EoftheITActprescribes punishmentforviolation ofprivacyandprovides that anyperson whointentionallyor knowinglycaptures, publishes or transmitstheimageof aprivateareaof anypersonwithout his orher consent,undercircumstancesviolatingtheprivacyofthatperson,shallbepunishedwithimprisonmentwhichmayextendto3(three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.

ThereisnoprovisionintheIPCthatmirrorsSection66EoftheITAct,thoughsections292and509oftheIPCdocoverthisoffencepartially.

Section 292 of theIPC has been discussed above. Section 509 of theIPC provides that if anypersonintending toinsult the modestyofanywoman,utters anyword,makes anysoundorgesture,orexhibits anyobject,intendingthatsuchwordorsound shall beheard,orthatsuchgestureorobjectshallbeseen,bysuchwoman,orintrudesupontheprivacyofsuchwoman,suchpersonshall bepunished with simple imprisonment for a term which may extend to 1 (one) year, or with fine, or with both. Unlikesection66EoftheITActwhichappliestovictimsofbothgenders,section509oftheIPCappliesonlyifthevictimisawoman.

Section67CoftheIT Act: Section67CoftheITActrequires an'intermediary'topreserveandretainsuchinformationasmay be specified for such duration and in such manner and format as the Central Government may prescribe. Thesection further provides that any intermediary who intentionally or knowingly contravenes this requirement shall be punished with imprisonmentfor atermwhichmayextendto3(three) years andalsobeliabletoafine. An'intermediary' withrespecttoany particular electronic record, has been defined in theIT Act tomean anyperson who on behalf of another personreceives, stores or transmits that record or provides anyservice with respect to that record and includes telecomservice providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes. There is no corresponding provision in the IPC.

Cyber terrorism: Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, with intent to threaten the unity, integrity,securityorsovereigntyofIndiaortostriketerrorinthepeopleoranysectionofthepeople, denies orcausesthe denial of access to any person authorized to access a computer resource, or attempts to penetrate or access acomputer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of anycomputer contaminant, andby meansof suchconductcauses oris likelytocausedeath or injuries to persons or damageto ordestruction of property or disruptsor knowing that it islikelyto causedamage or disruption of suppliesor servicesessential to the life of the community or adversely affect critical information infrastructure, is guilty of 'cyber terrorism'. Whoever knowinglyor intentionally penetrates or accesses acomputer resource without authorisation or exceeding authorised access, and bymeans of suchconductobtains accesstoinformation,dataor computer databasethatisrestrictedforreasonsforthesecurityoftheState or foreign relations,or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used tocause or likely to cause injury to the interests of the sovereignty and integrity of India, thesecurityoftheState, friendlyrelations withforeign States, public order, decencyor morality, orin relation tocontempt of court, defamation or incitement toan offence, or tothe advantage of anyforeign nation, group of individuals or otherwise, is also guilty of 'cyber terrorism'.

Whoevercommits orconspirestocommitcyberterrorismshallbepunishablewithimprisonmentwhichmayextendto imprisonmentfor life.

ThereisnoprovisionintheIPCthatmirrorssection66FoftheITAct,thoughsection121oftheIPC(waging,orattemptingtowagewar, or abetting waging of war, against the Government of India) does cover this offence partially.

WhetherCompoundable,CognizableandBailable
Section77AoftheITAct providesthat,subjecttocertainexceptions, alloffences undertheITActforwhichthepunishmentis imprisonmentforatermof3(three)yearsorless,arecompoundable. Theprovisionsofsections265B and265Cof theCodeof Criminal Procedure, 1973 ("CrPC") shall apply with respect to such compounding.

Section 77B of the IT Act provides that notwithstanding anything contained in the CrPC, all offences punishable with imprisonmentof3(three)yearsandaboveundertheITActshallbecognizableandalloffencespunishablewithimprisonmentof3 (three) years or less shall be bailable.

Mostofthecyber-crimescoveredundertheITActarepunishablewithimprisonmentof3(three)yearsorless.Thecyber-crimes which are punishable with imprisonment of more than 3 (three) years are:

a. publishingortransmittingobscenematerialinelectronicformundersection67oftheITAct;
b. publishingortransmittingofmaterialcontainingsexuallyexplicitact,etc.,inelectronicformundersection67AoftheITAct;
c. publishingortransmittingofmaterialdepictingchildreninsexuallyexplicitact,etc.,inelectronicformundersection67Bof the IT Act; and
d. cyberterrorismundersection66FoftheITAct.

All of the cyber-crimes under the IPC are bailableother than offences under section 420 (*cheating and dishonestly inducing delivery of property*), section 468 (*forgery for the purpose of cheating*), section 411 (*dishonestly receiving stolen property*), section378(*theft*)andsection409(*criminalbreachoftrustbypublicservant,orbybanker,merchantoragent*),whicharenon-bailable.

Offences under sections 463 and 465 (*forgery*), sections 425 and 426 (*mischief*), section 468 (*forgery for the purpose of cheating*),section469(*forgeryforthepurposeof harmingreputation*)andsection292(*sale,etc., of obscenebooks,etc.*)ofthe IPCarenon-compoundableoffenceswhileoffencesundersections378and379(*theft*),420(*cheatinganddishonestlyinducingdelivery of property*), sections 425 and 426 (*mischief when the only loss or damage caused is loss or damage to a private person*), section 509 (*word, gesture or act intended to insult the modesty of a woman*), section 411 (*Dishonestly receivingstolen property*)andsection419(*Punishmentforcheatingbypersonation*)oftheIPC arecompoundableoffences.Ofthese,offences undersections 420and509canbecompoundedonlywiththepermissionofthecourt.Mostofthecybercrimesunder the IPC are cognizable other than the offences under sections 425 and 426 (*mischief*) and sections 463 and 465 (*forgery*)which are non-cognizable.

The overlap between the provisions of theIPC and theIT Act maysometimes lead to an anomalous situation wherein certain offences arebailableunder theIPC and not under the IT Act and vice versaandcertain offences arecompoundableunder the IPCandnot undertheITAct andviceversa.Forinstance,incaseof hackinganddata theft,offencesundersections43and66 of the ITAct that arebailable and compoundable while offences under section 378 of theIPC are non-bailable and offences under section 425 of theIPC are non-compoundable. Further, in caseof the offence of receipt of stolen property, the offenceunder section66B of theIT Act is bailable whilethe offenceunder section 411 of theIPC is non-bailable. Similarly, incase of the offenceofidentitytheft andcheatingbypersonation,theoffencesundersections66C and66D oftheITActare compoundable and bailable while the offences under sections 463, 465 and 468 of theIPC are non-compoundable and the offences undersections 468and 420 of theIPC are non-bailable. Finally, incase of obscenity, the offences under sections 67, 67A and 67Bof the IT Act are non-bailable while the offencesunder section 292 and 294 of the IPC arebailable. Thisissuehas been dealt with by the Bombay High Court in the case of *Gagan Harsh Sharma v. The State of Maharashtra*[2] (discussed below) wherein offences under sections 408 and 420 of theIPC that are non-bailable and cannot be compounded other than withthepermissionofthecourtwereinconflictwithoffencesundersections43,65and66oftheITActthatarebailableand compoundable.

ConflictbetweentheIPCandtheITAct:CaseLaw
Inthecaseof*SharatBabuDigumartiv.GovernmentofNCTofDelhi*[3],theconflictbetweenprovisionsoftheIPCandtheITActcameto the fore. In this case, on November 27, 2004, an obscene video had been listed for sale on baazee.com("Bazee").
The listing was intentionally made under the category 'Books and Magazines' and sub-category 'ebooks' in order to avoid its detectionbythefiltersinstalledbyBaazee. Afewcopies weresoldbeforethelistingwas deactivated. LaterDelhi police'scrime branch charge-sheeted Avinash Bajaj, Bazee's managing director andSharatDigumarti, Bazee's manager.ThecompanyBazee was not arraigned as an accusedand this helpedAvinash Bajaj get off thehook sinceit was held that, vicarious liability couldnotbefastenedonAvinashBajaj undereithersection292oftheIPCorsection67oftheITActwhenAvinash's employer Bazee itselfwas notan accused.Later changesundersection 67 oftheITActandsection 294 ofIPCagainstSharatDigumarti were also dropped,but thechargesundersection292of theIPC wereretained. TheSupremeCourtthenconsideredif, after thecharges under section 67 of theIT Act was dropped, a charge under section 292 of the IPC could be sustained. The Supreme Court quashedtheproceedings againstSaratDigumartiandruled thatif an offenceinvolvesan electronic record,theIT Act alone would applysincesuch was thelegislative intent. It is asettled principle of interpretationthat special laws would prevail overgeneral laws andlatter laws would prevail overpriorlegislation. Further, section 81 of theIT Actstates that the provisions of theITAct shall haveeffect notwithstandinganything inconsistent therewith contained in any other lawfor thetime being in force.

In the case of *Gagan Harsh Sharma v. The State of Maharashtra*[4], certain individuals were accused of theft of data and software from their employer andcharged under sections 408and 420 ofthe IPC andalsounder sections 43,65 and 66ofthe IT Act. All of these sections, other than section 408 of theIPC, have been discussed above. Section 408 of the IPC deals with criminalbreachoftrust byclerkorservant andstatesthat"*whoever,beingaclerk orservant oremployedas aclerk orservant, andbeinginanymannerentrustedinsuchcapacitywithproperty,orwithanydominionoverproperty,commitscriminalbreachoftrustin respectofthatproperty,shallbepunishedwithimprisonmentofeitherdescriptionforatermwhichmay extendtosevenyears, and shall also be liable to fine*".

Offencesundersections408and420oftheIPC arenon-bailableandcannotbecompoundedotherthan withthepermission ofthe court. Offences under sections 43,65 and 66 of theIT Act arebailable and compoundable.Therefore,thepetitioners pleaded that thecharges against them under the IPC be dropped and the charges against them under the IT Act beinvestigatedandpursued.ItwasfurtherarguedthatiftheSupremeCourt's rulingin*SharatBabuDigumarti* weretobefollowed, the petitioners could only be charged under theIT Act and not under theIPC, for offences arising out of the same actions.

TheBombayHighCourtupheldthecontentionsofthepetitionersandruledthatthechargesagainstthemundertheIPCbedropped.

ASuitableHomeforCyber Offences
Wecurrently have a situation where a number of offences are penalised byboth the IPC and the IT Act, even though the ingredients of both offences are the same. There are subtle differences in punishments under these statutes, especiallyin aspects likewhether the offenceis bailable or compoundable or cognizable. An offencesuch as obscenity may take place throughdifferenttypesofmedia,bothonlineoroffline.However,itcouldresultinunfairnessif2(two)differentstatutesapplytothesame offence on the basis of the media used.

The sum and substance of theSupreme Court's ruling in the *SharatBabu Digumarti* caseis that noindividual may be charged under theIPC for an offencearising out of certain acts or omissions if theIT Act could alsobe applied tothesame acts or omissions.ThoughweareinfullagreementwiththeSupremeCourt'sruling,itisourcontentionthatallcyberoffencesoughttobehoused in the IPC and not in the IT Act. The "cyber" component of an offence is not sufficient reason for differential treatment of sub-categories of the offence. Even though the supreme court's ruling in the *Sharat Babu Digumarti* case has ensured that no individual may becharged under theIPC for an offencearising out of certain acts or omissions if theIT Act could alsobe applied to thesame acts or omissions, it is a fact that offences such as theft and obscenitywill bepunished differentlyifthey involve a 'cyber' element. Currently, an individual who distributes a hard copy book containing obscene materials will be punished under theIPC whilst an individual who distributes obscenematerials through theinternet will bepunished under the IT Act, though theunderlying offenceisthe same. A personwho stealsacarwill be punished under the IPC whilstan individual who indulges in theft of online data will be punished under the IT Act.

Theftistheft,irrespectiveofwhetherthestolenpropertyisdigitalorphysical.Obscenitytransmittedthroughtheinternetshouldbetreated at par with obscenity which is transmitted offline.

IPC'streatmentofstalking
The legislature's treatment of the offenceof "stalking", accomplished through the insertion of new section 354D in the IPC throughtheCriminalLaw(Amendment)Act,2013[5],is acaseinpoint.Section354Dpenalisestheoffenceof"stalking" whetherit has acybercomponentornot.Ifamanfollows awomanandcontacts,orattemptstocontact,suchwomantofosterpersonal interaction repeatedlydespiteaclear indication ofdisinterestbysuchwoman,it amountstostalking.If amanmonitorstheusebyawoman of the internet, email or any other form of electronic communication, it will alsoresult in the offenceof stalking. Thereareafewexemptionstothisoffenceofstalking, andallthedefencesapplyirrespectiveof whetherthestalkingiscyberstalking or not.ThepunishmentprescribedforstalkingbySection354D of theIPCdoes notdiscriminateonthebasis ofthepresenceor absence of the "cyber" component.

AmendmentstotheIPCtocovercyber-crimes
TheIndianlegislaturehasfromtimetotime,madeanumberofamendmentstotheIPC,tospecificallycovercyber-crimes.Someofthe important amendments are as follows:

a. anewsection29Awascreatedtodefine"electronicrecord"bylinkingitwiththedefinitiongivenintheITAct[6];
b. a new sub-section (3) was inserted in section 4 of the IPC (relating to the extension of theIPC toextra territorial offences)thatstatesthattheprovisionsoftheIPCshallbeapplicabletoanypersoninanyplace"*withoutandbeyondIndia*", committing an offence targeting a computer resource located in India[7];

c. in sections 118and 119 of the IPC(that deal with the concealment of a design tocommit anoffencepunishable with death or imprisonment for lifeand a public servant concealing a design tocommit an offence which it is his dutyto prevent,respectively),thewords "*voluntarilyconcealsbyanyactoromission orbytheuseofencryptionorany other informationhidingtool,theexistenceofadesign*" wereinsertedbeforethewords"*tocommitsuchoffenceor makes any representation which he knows to be false respecting such design*"[8];

d. in section 464 of the IPC (which penalises the making of a false document), the phrase"digital signature" was replacedwiththephrase"electronicsignature"inallplaces.Thesectionwas alsoamendedtoincludethemakingof false electronicrecordsandaffixingelectronicsignaturesunderitsambitandthephrase"affixingelectronicsignature" was given the same meaning as it has under the IT Act[9];

e. "electronicrecord" wasincludedwithintheambitofsections164,172,173,175,192,204,463,466,468,469,470, 471,474and476oftheIPCthatearlieronlyprovidedfor"documents","books","paper","writing"or"records",asthecasemay be;

f. insection466oftheIPC(whichdeals withforgery ofcourtrecords or ofpublicregisters),theterm"register" was definedtoincludeanylist,dataorrecordofanyentriesmaintainedinan"electronicform",asdefinedinsection2(1) (r)oftheITAct[10];and

g. anewsection354DwasinsertedintheIPCthatintroducestheoffenceofcyberstalking,whichhasbeendiscussedabove.

Badandill-thoughtoutdrafting

Article14oftheConstitutionofIndia,1950("Constitution")statesthattheStateshallnotdenytoanypersonequalitybeforethelaworthe equalprotection of thelaws within theterritory of India. It is not our contention that thecurrent stateof affairs results inaperseviolationofArticle14oftheConstitutioneventhoughit hascreatedanunhappystateof affairs.Thelegislaturedoes have the freedom tomakespecific laws forspecific matters orsituations.However, thedocking of cyber-crimes in theIT Act does not appear to have been well thought through.

When the IT Act was enacted, its focus was on putting in place technologylaw fundamentals like digital signatures, providing legalrecognitionforelectronic documents andthelike.Itspreamblestatedthatits objectivewasto"*provide legalrecognitionfor transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storageofinformation,tofacilitateelectronicfilingof documentswiththeGovernment agencies andfurthertoamendtheIndian Penal Code,the IndianEvidenceAct,1872, theBankers'Books Evidence Act,1891 andthe ReserveBank of India Act, 1934and for matters connected therewith or incidental thereto.*"[11]

EventhoughtheITAct penalisedcyber-crimeswithabroadbrushthroughsections43,66and67, it was onlyin2008thatthe IT Act was amended[12] and provisions were made for specific cyber-crimes such as sending offensive messages through communication servers, dishonestly receiving a stolen computer resource or communication device, identity theft, violation of privacy, cyber terrorism etc.throughsections66Ato66Fandsections 67Ato67C.Theseamendmentsstick outlikeanunwieldyappendage.

Therefore,itissubmittedthatallcyberoffencesintheITActoughttoberepealedandtheIPCbesuitablymodified(tocoverallofthecyber-crimes, including those currently covered under the IT Act) at the earliest possible convenience of the legislature.

RelevantSectionsofIndianEvidenceAct:

AmendmentsrelatedtotheevidenceActwerecontainedinSec.92andthe SecondScheduleoftheITAct,2000.PursuanttotheenactmentoftheInformation Technology (amendment) Act, 2008, Sec.92 was deletedandtheprovisionswithregardtotheIndianEvidenceActwerementionedinPartIVoftheamendmentAct.

1) AmendmentofSec.3–
Insection3relatingtointerpretationclause,intheparagraphappearingattheend,forthewords"digitalsignature"and"DigitalSignatureCertificate",the words "Electronic signature" and "Electronic Signature Certificate" shall be respectively substituted.

2) InsertionofnewSec.45A–OpinionofExaminerofElectronicevidence–45A:
When in a proceeding, the Court hasto form an opinion on any matter relating to any information transmitted or stored in anycomputerresourceoranyother electronicor digital form,theopinionofthe Examiner ofElectronicEvidencereferredtoinsection79AoftheInformationTechnologyAct,2000,isarelevantfact.Explanation:Forthepurposesofthissection, anExaminerofElectronicEvidenceshallbeanexpert

3) AmendmentofSec.47A–
Insection47A,-
(i)forthewords"digitalsignature",thewords"electronicsignature"shallbesubstituted;(ii)forthewords"DigitalSignatureCertificate", the words "Electronic Signature Certificate" shall be substituted.

4) AmendmentofSec.67A–
Insection67A,-forthewords"digitalsignature",thewords"electronicsignature"shallbesubstituted.

5) AmendmentofSec.85A–
Insection85A,forthewords"digitalsignature",wherevertheyoccur,thewords"electronicsignature"shallbesubstituted.

6) AmendmentofSec.85B–
Insection85B,-forthewords"digitalsignature",wherevertheyoccur,thewords"electronicsignature"shallbesubstituted.

7) AmendmentofSec.85C–
Insection85C,forthewords"DigitalSignatureCertificate",thewords"ElectronicSignatureCertificate"shallbesubstituted.

8) AmendmentofSec.90A–
Insection90A,thewords"digitalsignature",atbothplaceswheretheyoccur,thewords"electronicsignature"shallbesubstituted.

RelevantSectionsofReserveBankofIndiaAct:

TableofContents

Introduction

Maintaining recordsisan integral andessentialpart of thebanking institutions. Forinstance, a customerwantsto deposit₹10000inabank.Hedepositstheamountwithabankerwhoacknowledgesthedepositwithareceipt. The banker will then make proper entry of the same in a ledger book or an account book. Later, the customer claims that he deposited₹15000 in the bank but only ₹10000 were credited in his account. In this case, the banker will have appropriate records to verify it. Thebank can verify that only ₹10000 weredeposited by the customer. If any legal proceedings are initiated against the bank, it can produce a certified copyoftherecord.TheBankers'BooksEvidenceAct,1891providesthelawwithrespecttobankers'booksand what are the certified copies of the bank records.

Historicaloverview

Records have been maintained in banking institutions since their inception. The procedure of maintaining records is integral for such establishments. These records are usually maintained in ledger books, account books,etc.thesearecalledbankers'books.TheBankers'BooksEvidenceBillwaspassedbythelegislatureon1stOctober 1891. The main objective of this Act was to make the provisions of the English Bankers' BooksEvidence Act, 1879in India.

InEngland,thislawwasbroughtintoforcetoamendtheLawofEvidencewithrespecttobankers'books. AccordingtothisAct,inalllegalproceedings,acopyofanyentryinthebankers'bookssuchas transactions, accountsshallbetreatedasaprimafacieevidenceof suchentry.

ThisActhasbeenamendedbytheInformationTechnologyAct,2000withtheadventofcomputersystemswhichare now being used to maintain records in banking institutions rather than on paper.

ImportanceofthisAct

the Bankers' Books Evidence Act 1891provides guidelines to banking institutions about legal proceedings relating to banking records. This is an Act which was brought into force to amend the Law of Evidence with respecttobanking records.Ineverybank,bookkeeping orrecording oftransactionsisrecorded inbank books suchasledgerbooks,registers,accountbooks,andotherbooksusedinordinarycoursesofbusiness. Ifthere isanydiscrepancyofthesebankingrecords,itwillamounttoaviolationunderthisAct.Anybankinginstitution or any company that carries out a banking function is bound by this Act if any legal proceeding is initiated against them.

Definitions

Section2oftheActdefinesthefollowing:

- **Company**:UnderthisAct,acompanyreferstoanycompanywhichisdefinedunder Section3ofthe CompaniesAct1956includinganyforeigncompanydefinedunderSection591ofthesameAct.

- **Corporation**:Anybodycorporateestablishedbyanylawfor thetimebeinginforceinIndiaisa corporation. ItincludestheReserveBankofIndia,theStateBankofIndiaandanysubsidiary bank as defined in the State Bank of India (Subsidiary Banks) Act 1959.

- **Bank/Banker**: According to this Act any company/corporation carrying on the business of bankingisabankorbanker.Further,itincludesanypostofficesavingsbank,anymoneyorderofficeand any partnership/ individual to whom the provisions of this Act have been extended.

- **Bankers'Books**:Thesereferto ledgerbooks,accountbooks,daybooks,cashbooks andother booksusedintheordinarycourseofbusinessofabank.Theserecordscanbekeptinawrittenformor they can be stored in microfilm, magnetic tape or any other form of mechanical or electronicdataretrievalmechanism.Theymaybekeptonsiteoratanoffsitelocationsuchasabackup or disaster recovery site.

- **Legal proceedings**: Under this Act, legal processing means any proceeding or inquiry under which evidence is given or may be given. It includes arbitration, any investigation/inquiry under theCriminalProcedureCode,1973oranyotherlawwhichis inforcefor thecollectionof evidencebyapoliceofficeroranyotherpersonauthorisedtodothesamebyamagistrateoranyexisting law.

- **TheCourt**:UnderthisAct,thecourtreferstotheperson(s)beforewhomthelegalproceedingsareheld.

- **Judge**:AJudgeunderthisActmeansaJudgeofaHighCourtDivision.

- **Trial**:ItreferstoanyhearingbeforetheCourtwhereevidenceistaken.

- **CertifiedCopy**:
  - With respect to written records, a certified copy means a copy of an entry in the bankers'bookwithacertificatewrittenatthefootofsuchcopy.Itcertifiesthatitisatrue copy of the entry and it is contained in ordinary books of banks, made in the ordinarycourseofbusinessandtheconcernedbookisstillinthecustodyof thebank. A copy can also be obtained mechanically or by any other process that itself ensures the accuracy of the copy, in this case, a certificate to that effect is also required. In certaincases,wherethebookfromwhichsuchcopywaspreparedisdestroyedintheusual course of business of the bank, a certificate to that effect is also required.These certificateshavetobedatedandsubscribedeitherbytheprincipalaccountant orthemanagerofthebankwithhisnameandofficial title.

  - When the books of records are stored as data in floppy, disk, tape or any other electromagneticdatastoragedevice thentheprintoutof suchdataorcopyofsuch printoutalongwithstatementscertifiedinaccordancewithSection2Aisacertifiedcopy.

  - Certifiedcopyalsoincludestheprintoutofanyentrythatisstoredinmicrofilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanismthatitselfensurestheaccuracyofsuchprintoutasacopyoftheentry and containing certificates in accordance with Section 2A.

Importantsectionsandsignificance

Section2

Section2AItprovidesthatcertaincertificatesshallbeaccompaniedwiththeprintoutorcopyofprintoutreferredin Section 2(8). They are:

- Certificatebytheprincipalaccountantofthebranchmanagerstatingthatitis:
  - Aprintoutoftheentryor
  - Acopyofsuchprintout
- Certificatebyapersoninchargeofthecomputersystemcontainingabriefdescriptionofthe computer system along with the following:
  - Particularsofsafeguardsadoptedbythesystemtoensurethatonlyauthorised persons have entered the data or performed any other information.

- Particularsofsafeguardsadoptedtoensurepreventionanddetectionofan unauthorised change of data.
- Particularsofsafeguardsavailabletoretrievelostdataduetoreasonssuchas systematic failure.
- Particularsofthemannerinwhichdataistransferredfromthesystemtoany removablemediasuchasfloppy,disc,tape,oranyotherelectromagneticdatastorage device.
- Particularsofthemodeofverificationensuringtheaccuratetransferofsuchdatato the removable media.
- Particularsofthemodeofidentificationofsuchdatastoragedevice
- Particularsofarrangementforcustodyandstorageofsuchdevices
- Particularsofthesafeguardstopreventanddetecttamperingwiththesystem
- Anyotherfactorwhichcancertifytheaccuracyandintegrityofthesystem.According to

Section 2A(c), acertificate is required from the person in chargeof the computer system that the computeroperatedproperlyatthematerialtimeastothebestof hisknowledgeandthathewasprovidedwith relevant data. It further certifies that the printout correctly represents or is derived from the relevant data.

Section3

Section 3states the power of the State Government to extend the provisions of this Act. The State Governmentcanextendtheprovisionsofthis Acttobeappliedtothebooksofanypartnershiporindividualcarryingon the businessof the bankerwithin territoriesthat fall underitsadministration. The State government can do so by notification in the official gazette and it can also rescind such notification.

Section4

Section4specifiescertainmatterswhichrequiretheproductionoforiginalentryforproperinvestigation. According tothissection,acertified copy ofanentryinabankers'book shallbeaprimafacieevidenceofthe existenceofsuchentry.Thecertifiedcopyshallbeadmittedasevidenceofmatters,transactionsandaccountsrecorded in every case. The certified copy shall be admissible to the same extent as an original copy is admissible.

Section5

Section5statesthatinlegalproceedingstowhichthebankisnotaparty,unlessthecourtor judgemakesan order for aspecialcause,theofficerofthebankshouldnotbecompelledtoeitherproducebankers'books forprovingany content or appear as a witness for proving matters, transactions, and accounts recorded.

Section6

Section6(1)providestheprovisionofinspectionofbooksbytheorderof thecourtorthejudge.Thecourtor judge may order:

- Apartytoalegalproceedingtobeatlibertytoinspectandtakecopiesofentriesinabankers' bookforpurposesofsuchproceedingor
- The bank to prepare and produce certified copies of all such entries within a specific time accompaniedbyacertificatedatedandprescribedintheprescribedmanner,statingthatnootherisfound in the books of the bank relating to the matter in an issue of the proceeding.

AccordingtoSection6(2),thecourtmayalsoorderunderSection5orSection6oftheActwithorwithout summoningthebankwhichshallbeservedonthebankthreedaysbeforethesameisrequiredtobeobeyed excluding bank holidays unless otherwise directed by the court or judge.

According to Section6(3),beforethe expiry of limited timefor theobedience of the aforementioned order, the bankmayatanytimeeitherofffertoproducethebooksof thebankatthetrial;orgive noticeoftheirintention to show cause against the concerned order which shall not be enforced without any further order.

Section7

According to Section 7(1),the costs of the application to the court or judge for the purpose of the Act and the costofanythingdoneortobedone undertheorderofcourtor judge,madefor thepurposeoftheAct shallbe atthediscretionofsuchcourtorjudge.Thecourtorjudgemayalsoordersuchcoststobepaidbythebanktoanypartyin case they have been incurred by any improper delay or fault of the bank.

AccordingtoSection7(2),suchorderofpaymentsofcoststoorbythebank shallbeenforcedonlyif thebank is apartyto the proceedings.

AccordingtoSection7(3)underSection7,anyorderonapplicationtotheCourtofCivilJudicatureawarding costsmaybe executed as ifitwereadecreefor moneypassedby itself.However,nothing inSection7(3)shall be construed to derogate from the power which is possessed by the court or judge making an order for enforcement of the directions relating to the payment of costs.

Section8

According to Section 8in the application of sections 5, 6 and 7 the investigation or inquiry under the CriminalProcedureCode,1973oranyotherlawwhichisinforcefor thecollectionofevidencebyapoliceofficerorany otherpersonauthorisedtodothesamebyamagistrateoranyexistinglaw,theorderofthecourtorjudge referred in sections 5, 6, and 7 shall be construed as referring to an order made by officers of rank Superintendent of Police or above as specified by the appropriate government. Here the appropriate government refers to the government which employs the police officer or any other person conducting the investigation or inquiry.

Amendments

TheInformationTechnologyAct,2000amendedthedefinitionofbankers'booksintheBankers'Books EvidenceAct,1891.ThefollowingchangesweremadebythisAct:

- Amendment in Section 2(3): Earlier the definition of bankers' books only contained ledgers, daybooks, cash books, accounts books as well as other books used in the ordinary course of businessinabank.Aftertheamendment,itincludesrecordsstoredinmicrofilm,magnetictapeorany other form of mechanical or electronic data retrieval mechanism.

- Section 2(8)(b): This sub-clause was added to the definition of a certified copy which includes a printoutofanyentrythatisstoredinmicrofilm,magnetictapeoranyotherformofmechanicalorelectronic data retrieval mechanism that itself ensures the accuracy of such printout as a copy of the entry

- Section 2A: This section was added to deal with certification requirements for admissibility of a certifiedcopyintheprintoutform.Itprovideswhichcertificatesshallberequiredbythepersoninchargeof the computer system.

Recentjudgements

Om Prakash v. Central Bureau of Investigation: In this case, it was held that Section 65B of the Indian Evidence Act is pari materia to Section 2Aof the Bankers' Books Evidence Act. Therefore they should be construed together. Moreover in *Anvar P.V v. P.K. Basheer and Ors*, it was observed that a special law will alwaysprevailovergenerallaw.This impliesthateventhoughthereisaprovision(Section65B)forelectronic records undertheIndianEvidenceAct,theprovisionthatdealsspecificallywiththeadmissibilityofbankingrecordsin electronic form are Section 2Aof the Bankers' Books Evidence Act. Thus, following the principle of 'generalia specialibus' Section 2Awill be preferred over Section 65 Bwith respect to dealing with banking records in electronic form.

*Sonu@Amarv.StateOfHaryana:*Inthiscase,itwasobservedthatthetesttodetermineanobjection pertainingtotheadmissibilityofbankingrecordsshouldbeallowedor notdependsonwhetherornotthe defectinquestioncouldbecuredatthestageofmarkingthedocumentandthepartytenderingevidencecouldhave resorted to the regular mode of proof.

Radheshyam G. Garg v. Safiya bai Ibrahim Lightwalla: In this case, it was observed that when an agent of banksignsacertificatevalidatingtherecordtobeatruecopyof theoriginal,maintainedintheusualcourse of business and kept in thebank'scustody then the court should not focuson all the conditionsprovided under Section 2(8)oftheActandtakeahyper-technicalapproach.Theconditionsprovidedunder Section2(8)oftheActare directory and not mandatory.

RelevantSectionsofIndianPenalCode(1860):

- **CHAPTERI**
  - INTRODUCTION
- **CHAPTERII**
  - GENERALEXPLANATIONS
- **CHAPTERIII**
  - OFPUNISHMENTS
- **CHAPTERIV**
  - GENERALEXCEPTIONS
    - OftheRightofPrivateDefense
- **CHAPTERV**
  - OFABETMENT
- **CHAPTERVA**
  - CRIMINALCONSPIRACY
- **CHAPTERVI**
  - OFOFFENCESAGAINSTTHESTATE
- **CHAPTERVII**
  - OFOFFENCESRELATINGTOTHEARMY,NAVYANDAIRFORCE
- **CHAPTERVIII**
  - OFOFFENCESAGAINSTTHEPUBLICTRANQUILLITY
- **CHAPTERIX**
  - OFOFFENCESBYORRELATINGTOPUBLICSERVANTS
- **CHAPTERIXA**
  - OFOFFENCESRELATINGTOELECTIONS
- **CHAPTERX**
  - OFCONTEMPTSOFTHELAWFULAUTHORITYOFPUBLICSERVANTS
- **CHAPTERXI**

- OFFALSEEVIDENCEANDOFFENCESAGAINSTPUBLICJUSTICE

- **CHAPTERXII**
  - OFOFFENCESRELATINGTOCOINANDGOVERNMENTSTAMPS

- **CHAPTERXIII**
  - OFOFFENCESRELATINGTOWEIGHTSANDMEASURES

- **CHAPTERXIV**
  - OFOFFENCESAFFECTINGTHEPUBLICHEALTH,SAFETY,CONVENIENCE,DECENCYANDMORALS

- **CHAPTERXV**
  - OFOFFENCESRELATINGTORELIGION

- **CHAPTERXVI**
  - OFOFFENCESAFFECTINGTHEHUMANBODY
    - Ofoffencesaffectinglife
    - OfthecausingofMiscarriage,ofInjuriestounbornChildren,oftheExposureofInfants,andoftheconcealmentofBirths
    - OfHurt
    - Ofwrongfulrestraintandwrongfulconfinement
    - OfCriminalForceandAssault
    - OfKidnapping,Abduction,SlaveryandForcedLabour
    - Sexualoffences
    - OfUnnaturaloffences

- **CHAPTERXVII**
  - OFOFFENCESAGAINSTPROPERTY
    - OfTheft
    - OfExtortion
    - OfRobberyandDacoity
    - OfCriminalMisappropriationofProperty
    - OfCriminalBreachofTrust
    - OftheReceivingofStolenProperty
    - OfCheating
    - OfFraudulentDeedsandDispositionsofProperty
    - OfMischief
    - OfCriminalTrespass

- **CHAPTERXVIII**
  - OFOFFENCESRELATINGTODOCUMENTSANDTOPROPERTYMARKS
    - OfPropertyandOtherMarks
    - OfCurrency-NotesandBank-Notes

- **CHAPTERXIX**
  - OFTHECRIMINALBREACHOFCONTRACTSOFSERVICE

- **CHAPTERXX**
  - OFOFFENCESRELATINGTOMARRIAGE

- **CHAPTERXXA**
  - OFCRUELTYBYHUSBANDORRELATIVESOFHUSBAND

- **CHAPTERXXI**

  - OFD EFAMATION
- **CHAPTERX XII**RIMINALINTIMIDATION,INSU
  - ORC LT**XIII**TTEMPTSOFCOMMITOFFE NDANNOYANCE
- **CHAPTERX** NCES
  - OFA

INDIANPENALCODE,1860*(Sections1to51*

Ch	Sectioncovered		Classi
ChI	**Section1to5**	Introduction	
ChII	**Section6to52**	GeneralExplanations	
ChIII	**Section53to75**	OfPunishments	
ChIV	**Section76to106**	GeneralExceptions*oftheRightofPrivateDefense*(Section96to106)	
ChV	**Section107to120**	OfAbetment	
ChVA	**Section120Ato120B**	CriminalConspiracy	
ChVI	**Section121to130**	OfOffencesagainsttheState	
ChVII	**Section131to140**	OfOffencesrelatingtotheArmy,NavyandAirForce	
ChVIII	**Section141to160**	OfOffencesagainstthePublicTranquility	
ChIX	**Section161to171**	OfOffencesbyorrelatingtoPublicServants	
ChIXA	**Section171Ato171I**	OfOffencesRelatingtoElections	
ChX	**Section172to190**	OfContempt'sofLawfulAuthorityofPublicServants	

ChXI	**Section191to229**	OfFalseEvidenceandOffencesagainstPublicJustice

ChXII	**Section230to263**	OfOffencesrelatingtocoinandGovernmentStamps
ChXIII	**Section264to267**	OfOffencesrelatingtoWeightandMeasures
ChXIV	**Section268to294**	OfOffencesaffectingthePublicHealth,Safety,Convenience,DecencyandMorals.
ChXV	**Section295to298**	OfOffencesrelatingtoReligion
ChXVI	**Section299to377**	OfOffencesaffectingtheHumanBody. OfOffencesAffectingLifeincludingmurder,culpablehomicide(Section299to311)OftheCausingofMiscarriage,ofInjuriestoUnbornChildren,oftheExposureofInfants,andofthe • OfHurt(Section319to338) • OfWrongfulRestraintandWrongfulConfinement(Section339to348) • OfCriminalForceandAssault(Section349to358) • OfKidnapping,Abduction,SlaveryandForcedLabor(Section359to374) • SexualOffencesincludingrapeandSodomy(Section375to377)
ChXVII	**Section378to462**	OfOffencesAgainstProperty • OfTheft(Section378to382) • OfExtortion(Section383to389) • OfRobberyandDacoity(Section390to402) • OfCriminalMisappropriationofProperty(Section403to404) • OfCriminalBreachofTrust(Section405to409) • OftheReceivingofStolenProperty(Section410to414) • OfCheating(Section415to420) • OfFraudulentDeedsandDispositionofProperty(Section421to424) • OfMischief(Section425to440) • OfCriminalTrespass(Section441to462)
ChXVIII	**Section463to489-E**	OffencesrelatingtoDocumentsandPropertyMarks • OffencesrelatingtoDocuments(Section463to477-A) • OffencesrelatingtoPropertyandOtherMarks(Section478to489) • OffencesrelatingtoCurrencyNotesandBankNotes(Section489Ato489E)
ChXIX	**Section490to492**	OftheCriminalBreachofContractsofService
ChXX	**Section493to498**	OfOffencesrelatedtomarriage
ChXXA	**Section498A**	OfCrueltybyHusbandorRelativesofHusband
ChXXI	**Section499to502**	OfDefamation
ChXXII	**Section503to510**	OfCriminalintimidation,InsultandAnnoyance
ChXXIII	**Section511**	OfAttempttoCommitOffences

RelevantSectionsofReserveBankofIndiaAct:

MASTERDIRECTIONS

(261kb)
MasterDirectiononDigitalPaymentSecurityControls

RBI/2020-21/74DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21

February18,2021

The Chairman/ Managing Director/ Chief ExecutiveOfficerAll Scheduled Commercial Banks excluding RRBs/SmallFinanceBanks/PaymentsBanks/CreditCardissuingNBFCs.

Madam/DearSir,

MasterDirectiononDigitalPaymentSecurityControls

PleaserefertoparaII(7)oftheStatement onDevelopmentaland RegulatoryPoliciesoftheBi-monthlyMonetaryPolicyStatement for2020-21datedDecember4,2020(extractgivenbelow).TheMasterDirectionprovidesnecessaryguidelinesfortheregulatedentitiestoset up a robustgovernancestructure andimplement common minimum standards of securitycontrols for digitalpayment productsandservices.

Yoursfaithfully,

(T.K. Rajan)
ChiefGeneralManager

DigitalPaymentSecurityControls

Goingbythepre-eminentrolebeingplayedbydigitalpaymentsystemsinIndia,RBIgiveshighestimportancetothesecuritycontrolsaroundit.NowitisproposedtoissueReserveBankofIndia(DigitalPaymentSecurityControls)Directions2020,forregulatedentitiestosetuparobustgovernancestructureforsuchsystemsandimplementcommonminimumstandardsofsecuritycontrolsforchannelslikeinternet,mobilebanking,cardpayments,amongothers.Whiletheguidelineswillbetechnologyandplatformagnostic,itwillcreateanenhancedandenablingenvironmentforcustomerstousedigitalpaymentproductsinmoresafeandsecuremanner.Necessaryguidelines will be issued separately.

Index

MasterDirectiononDigitalPaymentSecurityControlsINTRODUCTION

In exercise of the powers conferred by the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and PaymentandSettlementSystemsAct,2007,theReserveBank,beingsatisfiedthatitisnecessaryandexpedientinthepublicinterestso todo,hereby,issuesthe directions hereinafter specified.

CHAPTER –I

PRELIMINARY

1. ShortTitleandCommencement

a. ThesedirectionsshallbecalledtheReserveBankofIndia(DigitalPaymentSecurityControls)directions,2021.

b. Thesedirectionsshallcomeintoeffectsixmonthsfromthedaytheyareplacedontheofficial websiteoftheReserveBankofIndia (RBI).However, in respect of instructions already issued either by Department of Payment and Settlement Systems(DPSS),Department of Regulation (DoR) or Department of Supervision (DoS) of RBI including those to select RegulatedEntities(REs),bywayofcircular oradvisory,thetimelinewouldbe withimmediateeffector asper thetimelinesalreadyprescribed.

2. Applicability

TheprovisionsofthesedirectionsshallapplytothefollowingRegulatedEntities(REs):

a. ScheduledCommercialBanks(excludingRegionalRuralBanks);

b. SmallFinanceBanks;

c. PaymentsBanks;and

d. CreditcardissuingNBFCs.

3. Definitions

Allexpressionsunlessdefinedhereinshallhavethesamemeaningashavebeenassignedtothemunderthe BankingRegulationAct,1949,ReserveBankofIndiaAct,1934,PaymentandSettlementSystemsAct,2007orInformationTechnologyAct,2000/InformationTechnology(Amendment) Act,2008andRulesmadethereunder,anystatutory modification or re-enactment theretoor asusedincommercialparlance, as the case may be.

CHAPTER – II

GENERALCONTROLS

GovernanceandManagementofSecurityRisks

4. REs shall formulate a policy for digital payment products and services with the approval of their Board. The contours of thepolicy,whilediscussingtheparametersofany“newproduct”includingitsalignment with theoverallbusinessstrategyandinherent riskoftheproduct, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., shouldexplicitlydiscuss about payment security requirements from Functionality, Security and Performance (FSP) angles such as:

a. Necessarycontrolstoprotecttheconfidentialityofcustomerdataandintegrityofdataandprocessesassociatedwiththedigitalproduct/servicesoffered;

b. Availabilityofrequisiteinfrastructuree.g.humanresources,technology,etc.withnecessarybackup;

c. Assurancethatthepaymentproductisbuiltina securemannerofferingrobust performanceensuringsafety,consistencyandrolled out after necessary testing for achieving desired FSP;

d. Capacitybuildingandexpansionwithscalability(tomeetthegrowthforefficienttransactionprocessing);

e. Minimalcustomerservicedisruptionwithhighavailabilityofsystems/channels(tohaveminimaltechnicaldeclines);

f. Efficientandeffectivedisputeresolutionmechanismandhandlingofcustomergrievance;and

g. Adequateandappropriatereviewmechanism followedbyswift correctiveaction,incaseanyoneoftheaboverequirementsis hampered or having high potential to get hampered.

TheBoardandSeniorManagement shallberesponsibleforimplementationofthispolicy.Thepolicyshallbereviewedperiodically,atleast ona yearly basis.REsmayformulate thispolicyseparatelyforitsdifferentdigitalproducts orinclude the same aspartof theiroverallproductpolicy.Further,thepolicydocumentshouldrequirethateverydigitalpaymentproduct/servicesofferedaddressesthemechanics,cleardefinitionofstartingpoint,criticalintermittentstages/pointsandendpointinthedigitalpaymentcycle,securityaspects,validationstillthedigitalpaymentissettled,clearpictorialrepresentationofdigitalpathandexceptionhandling.Inaddition,signingoffoftheaboverequirements,mechanismforcarryingoutUserAcceptanceTests(UAT)inmultiplestagesbeforerollout,signofffrommultiplestakeholders(postUAT)anddataarchivalrequirementsshallalsobetakenintoaccount.Theneedforanexternalassessmentoftheentireprocessincludingthelogic,buildandsecurityaspectsoftheapplication(s)supportingthedigitalproductshouldbeclearlyarticulated.

5. REs shall incorporate appropriate processes into their governance and risk management programs for identifying,analysing,monitoringand managing the specific risks,including compliance risk and fraud risk,associated withthe portfolio of digitalpaymentproducts and services on a continual basis and in a holistic manner. The Board/ Senior Management of REs shall haveappropriateperformance monitoring systems/ key performance indicators for assessing whether the product or service offered throughdigitalpayment channels meet operational and security norms.

6. As part of this process, the REs shall define product-level limits on the level of acceptable security risk, document specificsecurityobjectivesand performance criteria including quantitative benchmarks for evaluating the success of the security built into thedigitalpaymentproductorservice,periodicallycompareactualresultswithprojectionsandqualitativebenchmarkstodetectandaddressadversetrends or concerns in a timely manner and modify the business plan/ strategy involving the product, when appropriate, based onthesecurity performance of the product or service.

7. REs shall have trained resources with necessary expertise to manage the digital payment infrastructure. Wherever the REsaredependentonthirdpartyserviceproviders,adequateoversightandcontrolsfor monitoringtheactivitiesof thethirdpartypersonnel,inlinewith RBI guidelines on outsourcing, shall be put in place.

8. REs shall conduct risk assessments with regard to the safety and security of digital payment products and associated processesandservices as well as suitability and appropriateness of the same vis-a-vis the target users, both prior to establishing the service(s)andregularly thereafter. The risk assessment should take into account –

a. Thetechnologystackandsolutionsused;

b. Knownvulnerabilitiesateachofthetouchpointsofthedigitalproductandtheremedialactiontakenbytheentity;

c. Dependenceonthirdpartyserviceprovidersandoversightoversuchproviders;

d. Riskarisingoutofintegrationofdigitalpaymentplatform withother systemsbothinternalandexternaltotheRE,includingcore systems and systems of payment systems operators, etc.;

e. Thecustomerexperience,convenienceandtechnologyadoptionrequiredtousesuchproducts;

f. Reconciliationprocess;

g. Interoperabilityaspects;

h. Datastorage,securityandprivacyprotectionasperextantlaws/instructions;

i. Operationalriskincludingfraudrisk;

j. Businesscontinuityandserviceavailability;

k. Compliancewithextantcybersecurityrequirements;and

l. Compatibilityaspects.

Such assessment shall cover the surrounding ecosystem as well. The assessment of risks shall address the need to protect andsecurepayment data[1]and evaluate the resilience of systems. The internal Risk and Control Self-Assessment (RCSA) exercise shallcover therisks (inherent) & controls vis-à-vis the probability and impact of threats to arrive at residual risk. In such an exercise, it isimperativefor REs to maintain database of all systems and applications storing customer data in the payment ecosystem andcompliance withapplicable PCI standards in each of the systems (notwithstanding mandatory requirements of certification/ standardaccreditation).

9. REs shall evaluate the risks associated with the chosen technology platforms, application architecture, both on the server andclientside. Further, REs should undertake a review of the risk scenarios and existing security measures based on incidents affectingtheirservices, before any major change to the infrastructure or procedures is made or, when, any new threats are identified throughriskmonitoring activities. Further, unused or unwanted features of the platform should be closely controlled to minimise risk.

10. REsshalldevelop soundinternalcontrolsystemsandtakeintoaccounttheoperationalriskbeforeofferingdigitalpayment productsandrelated services.This would include ensuring that adequate safeguardsare in place to protect integrity of data, customerconfidentialityand security of data.

11. REsshallensurethatthedigitalpaymentarchitectureisrobustandscalable,commensuratewiththetransactionvolumesandcustomergrowth.TheITstrategyoftheREshallensurethatarobustcapacitymanagementplanisinplacetomeetevolvingdemand.REsshallalsoputinplacereviewmechanismofIT/ITSecurityarchitectureandtechnologyplatformoverhaulonaperiodicbasisbased onBoard-approvedpolicy.

12. REsshallhavenecessarycapacity, systemsandproceduresinplacetoperiodicallytest thebacked-updata,applicationpertainingtodigitalproductstoensurerecovery withoutlossoftransactionsoraudit-trails.Thesefacilitiesshouldbetestedatleast ona half-yearlybasis fordigital payment products and services.

OtherGenericSecurityControls

13. The communication protocol in the digital payment channels (especially over Internet) shall adhere to a secure standard.Anappropriate level of encryption and security shall be implemented in the digital payment ecosystem.

14. Webapplicationsprovidingthedigitalpaymentproductsandservicesshouldnotstoresensitiveinformationin HTMLhiddenfields,cookies,or any other client-side storage to avoid any compromise in the integrity of the data.

15. REsshallimplementWebApplicationFirewall(WAF)solutionandDDoSmitigationtechniquestosecurethedigitalpaymentproducts and services offered over Internet.

16. Thekeylength (forsymmetric/ asymmetric encryption, hashing), algorithms(forencryption, signing, exchangeofkeys, creationofmessage digest, random number generators), cipher suites, digital certificates and applicable protocols used in transmissionchannels,processing of data,authentication purpose, shall be strong, adoptinginternationally accepted and published standardsthat arenotdeprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are ingeneral,compliant with extant instructions and the law of the land.

17. REsshallrenewtheirdigitalcertificatesusedindigitalpaymentecosystemwellintime.

18. Themobileapplication[2]andinternetbankingapplicationshouldhaveeffectiveloggingandmonitoringcapabilitiestotrackuseractivity, security changes and identify anomalous behaviour and transactions.

ApplicationSecurityLifeCycle(ASLC)

19. REsshallimplementmulti-tierapplicationarchitecture,segregatingapplication,databaseandpresentationlayerinthedigitalpayment products and services.

20. REsshallfollow a'securebydesign'approachinthedevelopmentofdigitalpaymentproductsandservices.REsshallensurethatdigital payment applicationsare inherently more secure by embedding security within their development lifecycle.

21. REsshallexplicitlydefinesecurityobjectives(includingprotectionofcustomerinformation/data)during(a)requirementsgathering,(b)designing,(c)development,(d)testingincludingsourcecodereview,(e)implementation,maintenance&monitoringand(f)decommissioning phases of the digital payment applications.

22. REs(includingthosepartneringwithotherentitiestoco-brand/co-developapplications)shalladoptandincorporateathreatmodelling approach during application lifecycle management into their policies, processes, guidelinesandprocedures.

23. Fordigitalpaymentapplicationsthatarelicensedbyathirdpartyvendor,REsshallhaveanescrowarrangementforthe sourcecodeforensuring continuity of services in case the vendor defaults or is unable to provide services.

24. REsshallconductsecuritytestingincludingreviewofsourcecode,VulnerabilityAssessment(VA)andPenetrationTesting(PT)oftheirdigitalpaymentapplicationstoassurethattheapplicationissecureforputtingthroughtransactionswhilepreservingconfidentialityandintegrityofthedatathatisstoredandtransmitted.SuchtestingshouldinvariablycovercompliancewithvariousstandardslikeOWASP.IfthesourcecodeisnotownedbytheRE,then,insuchcases,theREshallobtainacertificatefromtheapplicationdeveloperstatingthat the application is free of known vulnerabilities, malwaresand any covert channels in the code. In this context,

a. TheVAshallbeconductedatleastonahalf-yearlybasis;PTshallbeconductedatleastonayearlybasis.Inaddition,VA/PTshall be conducted as and when any new IT Infrastructure or digital paymentapplication is introduced or when any majorchange isperformed in application or infrastructure;

b. Testing related to review of source code/ certification shall be conducted/ obtained. This shall continue on a yearly basis,ifchanges/ upgrades have been made to the application during the year;

c. Testing/Certificationshouldbroadlyaddresstheobjectivethattheproduct/version/module(s)functionsonlyinamannerthatitisintendedtodo,isdevelopedasperthebestsecuredesign/codingpracticesandstandards,addressingknownflaws/threatsdue to insecurecoding;and

d. Penal provisions shall be included by the RE into third-party contractual arrangements for any non-compliance bytheapplicationprovider.

25. REs may also run automatedVA scanning tools to automaticallyscan allsystems onthe network that are critical,publicfacingorstore customer sensitive data on a continuous/ more frequent basis.

26. REsshallcomparetheresultsfromearliervulnerabilityscanstoverify/ascertainthatvulnerabilitiesareaddressedeitherbypatching,implementinga compensating control, or documentingandacceptingtheresidualrisk with necessary approvaland that thereis norecurrence ofthe known vulnerabilities. The identified vulnerabilities should be fixed in a time-bound manner.

27. REsshallensurethatallvulnerabilityscanningisperformedinauthenticatedmodeeitherwithagentsrunninglocallyonthesystemtoanalysethe security configuration or with remote scanners that are given administrative rights on the system being tested.[3]

28. REs shall verify and thoroughly test the functionality (to validate whether the system meets the functionalrequirements/specifications) and security controls of payment products and services before its launch/ moving to the productionenvironment.

29. REsshallinstituteamechanismtoactivelymonitorforthenon-genuine/unauthorised/maliciousapplications(withsimilarname/features) on popular app-stores and the Web and respond accordingly to bring them down.

30. TheserverattheRE'sendshouldhaveadequatechecksandbalancestoensurethatnotransactioniscarriedoutthroughnon-genuine/unauthoriseddigitalpaymentproducts/applicationsandtheauthenticationprocessisrobust,secureand centralised.

31. Thesecuritycontrols for digitalpayment applicationsmust focusonhowtheseapplicationshandle,storeandprotectpaymentdata.TheAPIsforsecuredatastorageandcommunicationhavetobeimplementedandusedcorrectlyinordertobeeffective.REsshallrefertostandardssuchasOWASP-MASVS,OWASP-ASVSandotherrelevantOWASPstandards,securityanddataprotectionguidelinesinISO 12812,threat catalogues and guides developed by NIST (including for Bluetooth and LTE security), for application security andotherprotection measures. Such testing has to necessarily verify for vulnerabilities including, but not limited to OWASP/ OWASPMobileTop 10, application security guidelines/ requirements developed/ shared by operating system providers/ OEMs.

32. REsshallredact/maskcustomerinformationsuchasaccountnumbers/cardnumbers/othersensitiveinformationwhentransmittedviaSMS/ e-mails.

AuthenticationFramework

33. In view of the proliferation of cyber-attacks and their potential consequences, REs should implement, except whereexplicitlypermitted/ relaxed, multi-factor authentication for payments through electronic modes and fund transfers, including cashwithdrawalsfrom ATMs/ micro-ATMs/ business correspondents, through digital payment applications. At least one of theauthenticationmethodologies should begenerallydynamicor non-replicable. [e.g., Use ofOne TimePassword, mobiledevices(devicebindingandSIM),biometric/ PKI/ hardwaretokens, EMV chip card(for CardPresent Transactions) with server-side verificationcouldbe termedeither in dynamic or non-replicable methodologies.].

34. REsmayalsoadoptadaptiveauthenticationtoselecttherightauthenticationfactorsdependingonriskassessment,userriskprofileandbehaviour.Properlydesignedandimplementedmulti-factorauthenticationmethodsaremorereliableandstrongerfrauddeterrentsandaremoredifficulttocompromise.Thekeyobjectivesofmulti-factorauthenticationaretoprotecttheconfidentialityofpaymentdataaswellasenhanceconfidenceindigitalpaymentbycombating variouscyber-attackmechanismslikephishing,keylogging,spyware/malwareandotherinternet-basedfraudstargetedatREsandtheircustomers. In this regard,

a. Theimplementationof appropriateauthenticationmethodologiesshouldbebasedonanassessmentoftheriskposedbytheRE'sdigitalpaymentproductsand services.Theriskshouldbeevaluatedinlightofthetypeofcustomer(e.g.,retail/corporate/commercial);thecustomertransactionalrequirements/pattern(e.g.,billpayment,fundtransfer),thesensitivityofcustomer information and the volume, value of transactions involved.

b. Beyondthetechnologyfactor,thesuccessofa particularauthentication methoddependsonappropriatepolicies,procedures,andcontrols. An effective authentication method should take into consideration customer acceptance, ease of use,reliableperformance,scalabilitytoaccommodategrowth,customerprofile,location,transaction,etc.,andinteroperabilitywithother systems.

c. To enhance online processing security, multi factor authentication and alerts (like SMS, e-mail, etc.) should be appliedinrespect of all payment transactions (including debits and credits), creation of new account linkages (addition/modification/deletionofbeneficiaries),changingaccountdetailsorrevisiontofundtransferlimits.Indevisingthesesecurityfeatures,REsshould take into account their efficacy and differing customer preferences for additional online protection.

d. The alerts and OTPs received bythe customer for online transactions shall identifythe merchant name, whereverapplicable,rather than the payment aggregator through which the transaction was effected.

e. Asanintegralpartofthemultifactorauthenticationarchitecture,REsshouldalsoimplementappropriatemeasurestominimiseexposuretoa middlemanattackwhichismorecommonlyknownasaman-in-the-middleattack(MITM),man-in-thebrowser(MITB)attackor man-in-theapplicationattack.This is to ensure,among other things,that thedata intransit is securedandthe transactionsare authenticated only by genuine/ authorised source/ process.

f. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction withthecustomer. Else, in the event of interference or in case the customer closes the application, the session should beterminated,andtheaffectedtransactionsresolvedor reversedout.Thecustomer should be promptly notifiedabout thestatusof thetransaction by email, SMS or through other means.

35. REs should set down the maximum number of failed log-in or authentication attempts after which access to the digitalpaymentproduct/ serviceisblocked.Theyshould havea secure procedureinplacetore-activatetheaccesstoblocked product/ service.Thecustomer shall be notified for failed log-in or authentication attempts.

FraudRiskManagement

36. The REsshalldocumentandimplementtheconfigurationaspectsforidentifyingsuspicious transactionalbehaviourinrespectofrules,preventive,detectivetypesofcontrols,mechanismtoalertthecustomersincaseoffailedauthenti cation, timeframe forthesame,etc.

37. Systemalertsshallbeparameterised and monitored intermsofvariousapplicableparameters. Such parameters, asapplicablecouldbe:transaction velocity(e.g., fund transfers, cash withdrawals, paymentsthrough electronic modes, addingnewbeneficiaries etc.)inashortperiod,moresointheaccountsofcustomerswho'veneverusedmobileapp/internetbanking/cardever(dependinguponthetypeofpa

ymentchannel), high risk merchant categorycodes (MCC) parameters, counterfeit card parameters (Stringof Invalid CVV/ PINsindicates anaccount generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations,IPaddressorigin(inrespectofunusualpatterns,prohibitedzones/rogueIPs),behaviouralbiometrics,transactionoriginationfrompointof compromise,transactionstomobilewallets/mobilenumbers/VPAsonwhomvishing fraudorothertypesoffraudis/areregistered/recorded, declined transactions, transactions with no approval code, etc.

38. Fraudanalysisshallbeconductedtoidentifythereasonforfraudoccurrenceanddeterminemechanismtopreventsuchfrauds.

39. Thestaff,especiallyinthefraudcontrolfunction,shallbeeducatedaboutfraudsandtrainedinthefollowingskillsandareasofexpertise:

a. Fraudcontroltoolsandtheirusage;

b. Investigativetechniquesandprocedures;

c. Cardholderandmerchanteducationtechniquestopreventfraud;

d. Scheme/Cardoperatingregulations;

e. Dataprocessingandanalysisandliaisingorcommunicatingwithlawenforcementagencies;and

f. Therequisiteskills requiredto(i)setandupdateappropriaterules, (ii)monitor theexceptionsthrown based ontherules onacontinuous basis and take necessary actions promptly, (iii) communicate/ escalate wherever required toappropriateauthorities, and (iv) differentiate false positives from the rest.

40. REs shallmaintain updated contact details of serviceproviders, intermediaries, externalagencies and other stakeholders(includingother REs) for coordination in incident response. REs shall put in place a mechanism with the stakeholders to update andverify suchcontactdetails.REsshallalsoformulatespecificSOPstohandleincidentsrelatedtopaymentecosystemtomitigatethelosseithertothecustomer or RE.

ReconciliationMechanism

41. Arealtime/near-realtime(notlaterthan24hoursfromthetimeofreceiptofsettlementfile(s))reconciliationframeworkforalldigitalpaymenttransactions between RE and allotherstakeholderssuchaspaymentsystemoperators,businesscorrespondents,cardnetworks,paymentsystemprocessors,paymentaggregators,paymentgateways,thirdpartytechnologyserviceproviders,otherparticipants,etc.,shallbeputinplaceforbetterdetectionandpreventionofsuspicioustransactions.Amechanismshallbeintroducedtomonitor the implementation and effectiveness of such framework.

CustomerProtection,AwarenessandGrievanceRedressalMechanism

42. REsshallincorporatesecure,safeandresponsibleusageguidelinesandtrainingmaterialsforenduserswithinthedigitalpaymentapplications. Theyshallalsomakeitmandatory(i.e. notprovidinganyoptiontocircumvent/avoidthematerial)fortheconsumertogothroughsecureusageguidelines(evenintheconsumer'spreferred language)whileobtainingandrecordingconfirmationduringtheon-boardingprocedureinthefirstinstanceandfirstuseaftereachupdateofthedigitalpaymentapplicationoraftermajorupdatestosecureand safeusageguidelines.

43. REsshallmention/incorporateasectiononthedigitalpaymentapplicationclearlyspecifyingtheprocessandprocedure(withforms/contactinformation,etc.)tolodgeconsumergrievances.Amechanismtokeepthisinformationperiodicallyupdatedshallalsobeputinplace.Thereportingfacilityontheapplicationshallprovideanoptionforregisteringagrievance.Customerdisputehandling,reportingandresolution procedures, including the expected timelines for the RE'sresponse should be clearly defined.

44. REsshalladheretoextantinstructions[4],updatedfromtimetotime,toputinplacesystem/sforonlinedisputeresolutionforresolvingdisputesand grievances of customers pertaining to digital payments.

45. REs shall educate customers about the need to maintain the physical and logical securityof their devices accessing digitalpaymentproducts and services including recommending secure/ regular installation of operating system and application updates,downloadingapplications only from authorised sources, having anti-malware/ anti-virus applications on devices, etc.

46. REsshallensurethatitscustomersareprovidedinformationabouttherisks,benefitsandliabilitiesofusingdigitalpaymentproductsanditsrelatedservicesbeforetheysubscribetothem.Customersshallalsobeinformedclearlyandpreciselyontheirrights,obligationsandresponsibilitiesonmattersrelatingtodigitalpayments, and, anyproblemsthat mayarisefromits serviceunavailability, processingerrorsand security breaches.The terms and conditions including customer privacy and security policy applying to digital paymentproducts and services shall bereadily available to customers within the product.All digital channels are to be offered on expresswillingness of customersand shallnot be bundled without their knowledge.

47. Whenever newoperating featuresor functions, particularlythose relating to security, integrityand authentication, are introducedtoonline delivery channels, clear and effective communication followed by sufficient instructions to properly utilise such newfeaturesshould be provided to the customers.

48. REs may continuously create public awareness on the types of threats and attacks used against the consumers while usingdigitalpayment products and precautionary measures to safeguard against the same. Customers shall be cautioned against commonlyknownthreats in recent times like phishing, vishing, reverse-phishing, remote access of mobile devices and educated to secure andsafeguardtheir account details, credentials, PIN, card details, devices, etc.

49. REsshallprovidedigitalpaymentproductsandservices,toacustomeronlyather/hisoptionbasedonspecificwrittenorauthenticated electronic requisition along with a positive acknowledgement of the terms and conditions.

50. REs should provide a mechanism on their mobile and internet banking application for their customers to, withnecessaryauthentication, identify/ markatransaction asfraudulent forseamlessand immediatenotificationtohisRE.Onsuchnotificationbythecustomer,theREs mayendeavour tobuildthecapabilityfor seamless/instantreportingof fraudulenttransactionstothe correspondingbeneficiary/ counterparty's RE; vice-versa have mechanism to receive such fraudulent transactions reported fromother REs. Theobjective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace thetransaction trail andmitigate the loss to the defrauded customer at the earliest possible time.

ChapterIII

INTERNETBANKINGSECURITYCONTROLS

Inadditiontothecontrolsprescribedin ChapterII,thefollowinginstructionsareapplicabletoREsoffering/intendingtoofferinternetbanking facility to their customers:

51. Internet banking websites are vulnerable to authentication related brute force attacks/ application layer Denial of Service(DoS)attacks. Based on the RE’s individual risk/ vulnerability assessment on authentication-related attacks such as brute force/ DoSattacks,REs shall implement additional levels of authentication to internet bankingwebsite such asadaptive authentication, strongCAPTCHA(preferably with anti-bot features) with server-side validation, etc., in order to plug this vulnerability and prevent itsexploitation.AppropriatemeasuresshallbetakentopreventDNScachepoisoningattacksandforsecurehandlingofcookies.Virtualkeyboardoptionshould be made available.

52. Anonlinesessionshallbeautomaticallyterminatedafterafixedperiodofinactivity.

53. Secure delivery of password for login purpose shall be ensured. The password generated and dispatched by the RE should bevalidfor a limited period from the date of its creation. If the password is generated and dispatched by the RE, then, the user shallbecompulsorily required to change the password, on the first login.

54. When the internet banking application is accessed through external websites (eg: in case of payment of taxes, e-commercetransactions,etc.),the procedureforauthenticationandtheappearance/lookand feeloftheRE’sinternetbankingsiteshouldbe madeuniform as far as possible.

ChapterIV

MOBILEPAYMENTSAPPLICATIONSECURITYCONTROLS

InadditiontothecontrolsprescribedinChapterII,thefollowinginstructionsareapplicabletotheREsoffering/intendingtooffermobilebanking/ mobile payments facility to their customers through mobile application:

55. Ondetectionofanyanomaliesorexceptionsforwhichthemobileapplicationwasnotprogrammed,thecustomersshallbedirectedtoremovethecurrentcopy/instanceoftheapplicationandproceedwithinstallationofanewcopy/instanceoftheapplication.REsshallbeable to verify the version of the mobile application before the transactions are enabled.

56. SpecificControlsformobileapplicationsinclude:

a. Devicepolicyenforcement(allowingappinstallation/executionafterbaselinerequirementsaremet);

b. Applicationsecuredownload/install;

c. Deactivatingolderapplicationversionsinaphasedbuttimeboundmanner(notexceedingsix monthsfromthedateofreleaseof newerversion) i.e., maintaining only one version (excluding the overlap period while phasing out older version) of themobileapplication on a platform/ operating system;

d. Storageofcustomerdata;

e. Deviceorapplicationencryption;

f. Ensuringminimaldatacollection/apppermissions;

g. Applicationsandbox/containerisation;

h. Abilityto identifyremote access applications (tothe extent possible) and prohibit login access tothemobile application,asamatter of precaution; and

i. Codeobfuscation.

57. REsmayconsidertoperformvalidationonthesecurityandcompatibilityconditionofthedevice/operatingsystemandthemobileapplication to ensure that activities relating to the account are put through the mobile application in a safe and secure manner.

58. REsmayexplorethefeasibilityofimplementingacodethatchecksifthedeviceisrooted/jailbrokenpriortotheinstallationofthemobile application and disallow the mobile application to install/ function if the phone is rooted/ jailbroken.

59. Checksumofcurrentactiveversionofapplicationshallbehostedonpublicplatformsothatuserscanverifythesame.

60. REsshallensuredevicebindingofmobileapplication[5].

61. Consideringthat the additionalfactorof authentication andmobile applicationmayresideon thesamemobiledeviceinthecaseofmobile banking, mobile payments, REs may consider implementing alternativesto SMS-based OTP authentication mechanisms.

62. Themobileapplicationshould requirere-authentication whenever thedeviceor application remainsunused for a designatedperiodandeach time the user launches the application. Applications must be able to identify new network connections or connectionsfromunsecured networks like unsecured Wi-Fi connections and must implement appropriate authentication/ checks/ measures toperformtransactions under those circumstances.

63. Themobileapplicationshouldnotstore/retainsensitivepersonal/consumerauthenticationinformationsuchasuserIDs,passwords,keys,hashes, hardcodedreferences onthe device andtheapplication should securely wipeany sensitive customer information frommemorywhen the customer/ user exits the application.

64. REsshallensurethattheirmobileapplicationlimitthewritingofsensitiveinformationinto‘temp’files.Thesensitiveinformationwritten in such files must be suitably encrypted/ masked/ hashed and stored securely.

65. REsmayconsiderdesigninganti-malwarecapabilitiesintotheirmobileapplications.

66. REsshallensurethattheusageofraw(visible)SQLqueriesinmobileapplicationstofetchorupdatedatafromdatabasesisavoided.MobileapplicationsshouldbesecuredfromSQLinjectiontypeofvulnerabilities.Sensitiveinformationshouldbewrittentothedatabaseinanencryptedform.Webcontent,aspartofthemobileapplication’slayout,shouldnotbeloadedifferrorsaredetectedduringSSL/TLSnegotiation.Certificateerrorsonaccountofthecertificatenotbeingsignedbyarecognisedcertificateauthority;expiry/revocationofthe certificate must be displayed to the user.

ChapterV

CARDPAYMENTSSECURITY

InadditiontothecontrolsprescribedinChapterII,thefollowinginstructionsareapplicabletotheREsoffering/intendingtoissuecards(credit/debit/ prepaid) (physical or virtual) to their customers:

67. REs shall follow various payment card standards (over and above PCI-DSS and PA-DSS[6]) as per Payment Card Industry(PCI)prescriptions for comprehensive payment card securityasper applicability/ readinessofupdatedversionsofthestandards suchas–

a. PCI-PIN(securemanagement,processing,andtransmissionofpersonalidentificationnumber(PIN)data);

b. PCI-PTS(securityapprovalframeworkaddressesthelogicaland/orphysicalprotectionofcardholderandothersensitivedataatpointof interaction (POI) devices and hardware security modules (HSMs);

c. PCI-HSM(securingcardholder-authenticationapplicationsandprocessesincludingkeygeneration,keyinjection,PINverification,secure encryption algorithm, etc.); and

d. PCI-P2PE(securitystandardthat requirespayment cardinformationtobeencryptedinstantlyuponitsinitial swipeandthensecurely transferred directly to the payment processor).

68. REsshouldensurethatterminalsinstalledatthemerchantsforcapturingcarddetailsforpaymentsorotherwisearevalidatedagainstthePCI-P2PEprogramtousePCI-approvedP2PEsolutions;PoSterminalswithPINentryinstalledatthemerchantsforcapturingcardpayments(including the double swipe terminals) are approved by the PCI-PTS program.

69. Acquirersshallsecuretheircardpaymentinfrastructure(UniqueKeyPerTerminal –UKPTorDerivedUniqueKeyPerTransaction– DUKPT/ Terminal Line Encryption – TLE).

70. ThesecuritycontrolstobeimplementedatHSMare:

a. TheHSMsshouldhaveloggingenabled,thelogsmustthemselvesbetamperproof;

b. HSMcanbecomea singlepointoffailure.Thisneedstobe mitigatedby‘clustering’ for highavailabilityandensuresecurebackups;

c. AccesstotheHSMshouldbecontrolledthroughAccessControlLists(ACLs);

d. SeparateACLsshouldbemaintainedforeachindividualapplicationtoensureapplicationlevelisolation;

e. AllaccesstoHSMshouldbemanagedandmonitoredusingarobustPrivilegedIdentityandAccessManagementsolution;

f. Decryptionandvalidationofkeys,PINshouldbedoneatHSM;

g. CardPINgenerationandprintingshouldbedirectlyatsystemconnectedHSM;

h. CVVgenerationandvalidationshouldbedoneatHSM;

i. EnsureHSMisimplementedwithsecurePINblockformatwithcontrolstodisableoutputtingPINblockinweakerformat;

j. SecurekeymanagementforHSMs(suchasLMKs,etc.);and

k. SecurityofthephysicalkeysoftheHSMdeviceshouldbeproperlymaintained.

71. REsshallimplementthefollowingforimprovingthesecuritypostureoftheATM:

a. Implement securitymeasuressuchasBIOSpassword,disabling USBports,disablingauto-run facility,applyingthelatestpatches of operating system and other softwares, terminal security solution, time-based admin access, etc;

b. Implementanti-skimmingandwhitelistingsolution;and

c. Upgradeallthe ATMswith supportedversionsofoperatingsystem.UseofATMsthathaveunsupportedoperatingsystemsshall be prohibited.

72. REsshallensurerobustsurveillance/monitoringofcardtransactions(especiallyoverseascashwithdrawals)andsettingupofrulesand limitscommensuratewiththeirrisk appetites. REsshalltakeupwiththecardnetwork and/ orATM network asthecasemaybe, toputin placetransaction limitsat Card,BIN as well asat theRE level. Suchlimits shall be mandatorily set at the cardnetworkswitchitself.Limits could be mandated both for domestic as well as international transactions separately. REs shall putin place transactioncontrolmechanisms with necessarycaps (restrictions on transactions), ifanyof the limitsset asper the aboverequirementisbreached.Aperiodicreviewmechanismofsuchlimitssetaspertheriskappetiteofthe REshallbeputinplace aspertheBoard-approvedpolicy.REsshallinstituteamechanismtomonitorbreaches,ifany,ona24x7basis,includingweekends,longholidaysandputinplacearobustincident responsemechanism to mitigate thefraud loss,on account of suspicioustransactions, if any. REsshall ensure thatcarddetailsofthe customersare not storedinplaintext at theRE anditsvendor(s) locations, systemsandapplications. REs shall alsoensurethattheprocessingofcarddetailsinreadableformatisperformedinasecuremannertostrictlyavoiddataleakageofsensitivecustomerinformation.

73. REsthatusecarddatascanningtoolstoidentifyunencrypted(cleartext)paymentscarddataintheirecosystemespeciallyduringaudits shall adhere to the following safety measures:

a. Anytool(procuredby/fromathird-party)forthepurposeofscanningofunencryptedcarddatashouldfirstbetestedinatestenvironment to understand the scope and impact of the tool’s capabilities;

b. ThescanningtoolshouldbeinstalledonlyintheRE'spremisesontheirdevices;

c. Carddatascanningshouldnotbedoneremotely;

d. Thediscovereddata,ifany,must preferablyresideinthescanningtool.Exportablecarddata must beappropriatelymasked.(No data, even masked, must be taken out of the RE’s premises/ infrastructure); and

e. LimitedaccesstoserviceproviderstoconductthescanoranalysethedataIfatall,mustbeprovidedonlyontheRE’sdevices.

Acronyms

ACL	AccessControlList

ASLC	ApplicationSecurityLifeCycle
ATM	AutomatedTellerMachine

BIN	BankIdentificationNumber
BIOS	BasicInput/OutputSystem
CAPTCHA	CompletelyAutomatedPublicTuringtesttotellComputersandHumansApart
CVV	CardVerificationValue
DDoS	DistributedDenialofService
DNS	DomainNameServer
DoR	DepartmentofRegulation
DoS	DepartmentofSupervision
DPSS	DepartmentofPaymentandSettlementSystems
DUKPT	DerivedUniqueKeyperTransaction
EMV	Europay,Mastercard,andVisa
FSP	Functionality,SecurityandPerformance
HSM	HardwareSecurityModule
HTML	HyperTextMarkupLanguage
IP	InternetProtocol
IT	InformationTechnology
IVR	InteractiveVoiceResponse
LMK	LocalMasterKey
MCC	MerchantCategoryCode
MITB	Man-in-TheBrowserattack
MITM	Man-In-the-Middleattack
NIST	NationalInstituteofStandardsandTechnology
OEM	OriginalEquipmentManufacturer
OTP	OneTimePassword
OWASP	OpenWebApplicationSecurityProject
OWASP-ASVS	OpenWebApplicationSecurityProject–ApplicationSecurityVerificationStandard
OWASP-MASVS	OpenWebApplicationSecurityProject–MobileApplicationSecurityVerificationStandard
PA-DSS	PaymentApplicationDataSecurityStandard
PCI	PaymentCardIndustry
PCI-DSS	PaymentCardIndustry-DataSecurityStandard
PCI-HSM	PaymentCardIndustry-HardwareSecurityModule
PCI-P2PE	PaymentCardIndustry-PointtoPointEncryption
PCI-PTS	PaymentCardIndustry-PINTransactionSecurity
PIN	PersonalIdentificationNumber
PKI	PublicKeyInfrastructure
PoS	PointofSale
PT	PenetrationTesting
RBI	ReserveBankofIndia
RCSA	RiskControlSelf-Assessment
REs	RegulatedEntities
SIM	SubscriberIdentificationModule
SOP	StandardOperatingProcedure
SQL	StructuredQueryLanguage
SSL	SecureSocketLayer
TLE	TerminalLineEncryption
TLS	TransportLayerSecurity
UAT	UserAcceptanceTest
UKPT	UniqueKeyPerterminal
USB	UniversalSerialBus
VA	VulnerabilityAssessment
VPA	VirtualPaymentAddress
WAF	WebApplicationFirewall

[1] customerdata;customerandbeneficiaryaccountdetails;paymentcredentials;transactiondata;

[2] Mobilebanking,mobilepaymentapplicationsoftheregulatedentities

[3] SANSCriticalSecurityControls

[4] RBI/2020-21/21DPSS.CO.PDNo.116/02.12.004/2020-21circulardatedAugust6,2020on'OnlineDisputeResolution (ODR) System for Digital Payments'

[5] The device binding should be preferably implemented through a combination of hardware, software and service information.Incase,theREallowsmultipledevicestoberegistered,then,(a)theusermustbenotifiedofeverynewdeviceregistration on multiple channels such as registered mobile number, email or phone call and (b) in relation to the mobile application,RE must maintaina record of all registered devices, providing the user afacility todisablearegistered device.

[6] PCISecureSoftwareStandard,aPCIstandardwithinPCISoftwareSecurityFramework(SSF)willreplacePA-DSSasthe primary standard for securing payment software in 2022. (ref: PCI security standards website)

1.Cybercrime

1.1 Wouldanyofthefollowingactivitiesconstituteacriminaloradministrativeoffenceinyourjurisdiction?Ifso,pleasepr ovide details of the offence, the maximum penalties available, and any examples of prosecutions inyourjurisdiction:

Hacking(i.e.unauthorisedaccess)

HackingisacriminaloffenceinIndiaandmayalsoleadtocivilliabilities.

Section43oftheInformationTechnologyAct, 2000(the"IT Act") proscribes, inrespectofacomputer,computersystem,computernetwork or computer resource: unauthorised access; unauthorised downloads, copies or extraction ofanydata, informationorcomputer database;introductionof"computer contaminants"orviruses; assistanceofany personinorderto facilitate access incontravention to the IT Act;and any manipulation ortampering thatcauses services availed byone persontobe charged toanother.

Prior to amendments to the IT Act in 2008, section 66 of said Act specifically defined hacking as the destruction, deletionoralterationofanyinformationresidinginacomputerresource,orthediminishmentofthevalueorutilityofacomputerresource,oranaction that affects a computer resource injuriously.These actions are now within the purview of section 43 of the IT Act as amendedin2008,whichnolongermakesspecificreferencetotheterm“hacking”butotherwiseretainsthelanguageoftheformersection6 6.Finally,section43 as amendedalsoproscribes thestealing,concealment, destruction oralteration (orcausing anypersontodoany of the foregoing) of any computer source code used for a computer resource with an intention to cause damage.

Thosefoundguiltyofoffencesundersection43shallbepunishablebyimprisonmentforatermofuptothreeyears,afineofINR500,000,or both.

Denial-of-serviceattacks

Denial-of-service(DoS)attacksarealso punishableundersection43oftheITAct.Any person, who,withoutpermissionoftheownerof a computer, computer system or computer network disrupts or causes disruption of said computer, computer systemorcomputernetwork,and/or deniesor causesthe denialofaccesstoanypersonauthorisedtoaccessanycomputer,computer systemorcomputernetworkby any means,ispunishableundersections43(e)and(f).Asindicatedpreviously,contraventionoftheprovisionsof section 43 is punishable by imprisonment for a term of up to three years, a fine of INR 500,000, or both.

Phishing

Thestatutedoesnotmakeexplicitreferencetophishing.However,in *NationalAssociationofSoftwareandServicesCompaniesv.AjaySood* 2005 (30) PTC 437 (Del), the Delhi High Court defined phishing as “…a form of internet fraud…” involving adeliberatemisrepresentationortheftofidentityin order to perpetrate theftofdata.Section 43oftheIT Actbroadlycoversactionswithinthisdefinition,whichmaybecategorisedasphishingattacks,asindicatedinpreviousanswers.Penaltiesforcontraventionofsection43havealso been specified above.

In addition, section 66C of the Information Technology (Amendment) Act, 2008 (the “IT Amendment Act”) states thatwhoeverfraudulentlyordishonestly makesuseoftheelectronicsignature,passwordoranyother uniqueidentificationfeatureofanyotherperson,shallbepunishedwithimprisonmentofuptothreeyears,andwillalsobe liable toa fineofuptoINR100,000.Section66Dof theITAmendmentAct prescribes the same penalties for whoever,by meansofanycommunication device orcomputerresourcecheats bypersonation.

InfectionofITsystemswithmalware(includingransomware,spyware,worms,trojansandviruses)

Section43oftheITActmakesitanoffenceforaperson,withoutthepermissionoftheownerofacomputer,computersystem,orcomputernetwork, to introduce or cause to be introduced any computer contaminant or computer virus into said computer,computersystem or computer network.

Theexplanationtosection43defines“computercontaminant”as“anysetofcomputerinstructionsthataredesigned–

(a) Tomodify,destroy,record,transmit,dataorprogrammeresidingwithinacomputer,computersystemorcomputernetwork;or

(b) Byanymeanstousurpthenormaloperationofthecomputer,computersystemorcomputernetwork".

The explanation defines "computer virus" as "any computer instruction, information, data or programme that destroys,damages,degradesor adverselyaffectsthe performanceofacomputerresourceor attachesitselftoanothercomputerresourceandoperateswhenaprogramme, dataorinstructionisexecutedorsomeothereventtakesplaceinthatcomputerresource".Penalties for thecontravention of section 43 are indicated above.

Distribution,saleorofferingforsaleofhardware,softwareorothertoolsusedtocommitcybercrime

TheITActdoesnotcontainclausesdirectlyreferringtodistribution,saleorofferingforsaletoolsforuseinthecommissionofcybercrime.

However,variousprovisionsofsection43penalise,inrespectofacomputer,computersystemorcomputernetwork,apersonwho:securesun authorised access; causes computer contaminants and/or viruses to be introduced; causes damage; causesdisruption;and/orcausesthe denialofaccess of anyauthorised persons.Additionally,section 43(g) proscribesthe provisionofanyassistancetoany persontofacilitateaccesstoa computer,computer systemorcomputer networkincontraventionoftheITAct.Penalties forthe contravention of section 43 are indicated above.

Inaddition,section84BoftheITAmendmentActalsoproscribestheabetmentofanyoffenceundertheITActortheITAmendmentAct.Thestat utestatesthatifno expressprovisionismadeforthepunishmentofsuchabetment, thepenaltythereonwillbethepunishmentprovided by the Act for the offence itself.

Possessionoruseofhardware,softwareorothertoolsusedtocommitcybercrime

TheITActdoesnotcontainclausesdirectlyreferringtopossessionoftoolsforuseinthecommissionofcybercrime.Seetheanswerunderthehe ading "Distribution, sale or offering for sale…" above.

Section 66B of the IT Amendment Act states that whoever dishonestly receives or retains any stolen computer resourceorcommunicationdeviceknowingorhavingreasontobelievethesametobe astolencomputerresourceorcommunicationdeviceshall bepunished with imprisonment of up to three years, a fine of up to INR 100,000, or both.

Identitytheftoridentityfraud(e.g.inconnectionwithaccessdevices)

Seetheanswerundertheheading“Phishing”above.

Electronictheft(e.g.breachofconfidencebyacurrentorformeremployee,orcriminalcopyrightinfringement)

Seetheanswerundertheheading“Hacking”above.

Unsolicitedpenetrationtesting (i.e.theexploitationofanITsystem withoutthepermissionofitsownertodetermineitsvulnerabilities and weak points)

Inadditiontotheoffencesdiscussedintheanswerundertheheading“Hacking”above,simplysecuringunauthorisedaccesstoacomputer,computer system, computer network or computer resource is punishable under section 43.This is punishable asindicated inprevious answers.However, the IT Act does not make specific reference to penetration testing.

Anyotheractivitythatadverselyaffectsorthreatensthesecurity,confidentiality, integrity oravailabilityofanyITsystem,infrastructure, communications network, device or data

Section66FoftheITAmendmentActdefinesandpenalisescyberterrorism.Theprovisionstatesasfollows:

“(1)Whoever–

(A) withintenttothreatentheunity,integrity,securityorsovereigntyofIndiaortostriketerrorinthepeopleoranysectionofthepeopleby—

(i) denyingorcausethedenialofaccesstoanypersonauthorisedtoaccesscomputerresource;or

(ii) attemptingtopenetrateoraccessacomputerresourcewithoutauthorisationorexceedingauthorisedaccess;or

(iii) introducingorcausingtointroduceanycomputercontaminant,

andby meansofsuchconductcausesorislikely tocause deathorinjuriesto personsordamagetoordestructionofpropertyordisruptsor knowingthatitislikelytocausedamageor disruptionofsuppliesorservicesessentialto the lifeofthecommunityoradversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorisedaccess,andbymeansofsuchconductobtainsaccesstoinformation,dataorcomputerdatabasethatisrestrictedforreasonsofthesecurity of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe thatsuchinformation, dataorcomputerdatabase soobtainedmaybeusedtocauseorlikelytocauseinjurytotheinterestsofthesovereigntyandintegrityofIndia,the securityoftheState, friendlyrelations withforeignStates,publicorder,decencyormorality,orinrelationtocontemptofcourt,defamationorincitementtoanoffence,ortotheadvantageofanyforeign nation, group of individuals orotherwise, commits the offence of cyber terrorism.

(2)Whoevercommitsorconspirestocommitcyberterrorismshallbepunishablewithimprisonmentwhichmayextendtoimprisonmentforlife."

1.2 Doanyoftheabove-mentionedoffenceshaveextraterritorialapplication?

AllprovisionsoftheITActandITAmendmentActapplytooffencesorcontraventionsoutsidetheterritoriesofIndiabyanyperson,ifsuchoffence or contravention should involve a computer, computer system or computer network located in India.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentionedoffences(e.g.wheretheoffenceinvolves"ethicalhacking",withnointenttocausedamageormakeafinancialgain)?

No,therearenot.

2. CybersecurityLaws

2.1 *ApplicableLaws*:Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity,includinglawsapplicabletothemonitoring,detection,prevention,mitigationandmanagementofIncidents. Thismayinclude,forexample,dataprotectionande-privacylaws,intellectualpropertylaws,confidentialitylaws,informationsecuritylaws,andimport/exportcontrols,amongothers.

1. TheITActandtheInformationTechnology(Amendment)Act2008

TheITActcontainsprovisionsfortheprotectionofelectronicdata.TheITActpenalises'cybercontraventions'(section43(a)–(h))and'cyberoffences' (sections 63–74).

TheITActwasoriginallypassedtoprovidealegalframeworkfore-commerceactivityandsanctionsforcomputermisuse,butnowalsoaddresses data protection and cybersecurity concerns.

2. TheInformationTechnologyRules(theITRules)

TheITRulesfocusonandregulatespecificareasofthecollection,transferandprocessingofdata,andincludethefollowing:

- TheInformationTechnology(Reasonable SecurityPractices andProceduresand SensitivePersonalDataorInformation)Rules,whichrequireentities holdingusers'sensitivepersonalinformationtomaintaincertainspecified security standards;
- TheInformationTechnology(GuidelinesforIntermediariesandDigitalMediaEthicsCode)Rules,2021,whichprohibitcontent ofaspecific natureontheinternet,andgoverntheroleof intermediaries,includingsocialmediaintermediaries, in keeping personal data of their users safe online;
- TheInformationTechnology(GuidelinesforCyberCafe)Rules,whichrequirecybercaféstoregisterwitharegistration agency and maintain a log of users' identities and their internet usage; and
- TheInformationTechnology(ElectronicServiceDelivery)Rules,whichallowtheGovernmenttospecifythatcertain services, such as applications, certificates and licences, be delivered electronically.

Proposedspecific dataprotectionlegislationinthe formofthePersonalDataProtectionBill2019hadbeentabledinParliamentfordeliberationinlate2020,andthenagainin2021.Itwasthenwithdrawnbythe Government in early August 2022 and is being re-worked in view of concerns that it was too broad.However, in addition to thelegislation described above, enforcement may alsosometimes occur on the basis of the Copyright Act, 1957.Depending on thecircumstances,otherlegislation,suchastheIndianPenal Code, 1860,theCodeofCriminalProcedure,1973,theIndianTelegraphAct, 1885, the Companies Act, 1956 and theConsumer Protection Act, 1986, may also sometimes apply.

In particular, the Indian Penal Code contains provisions covering most aspects of criminal laws, for instance, in respect oftheft,fraud,identitytheftandintentionalcausationofdamage, whichmay,broadlyspeaking, applytocyberoffences.ItisworthnotingthattheIT Act 2000contains a *non-obstante* clause in section 81, statingthat provisionsof any other statute that may beinconsistentwith those of the IT Act are overridden by the IT Act.However, the IT Amendment Act clarifies that this does notrestrict anyperson from exercising any rights conferred under the Copyright Act, 1957, or the Patents Act, 1970.

2.2 *Criticaloressentialinfrastructureandservices*:ArethereanycybersecurityrequirementsunderApplicableLaws(inaddition to those outlined above) applicable specifically to critical infrastructure, operators of essential services,orsimilar, inyourjurisdiction?

There are no industry- or sector-specific statutes making direct reference to cybersecurity requirements for operators ofessentialservicesorcriticalinfrastructure.However,variousnationalandindustrybodies,someofwhichareestablishedandempoweredby statute,overseecyber-hygieneandmaintainindustrystandards.

The Data SecurityCouncilofIndia (DSCI)isa not-for-profitbodyestablishedbytheNationalAssociationofSoftwareandServicesCompanies(NASSCOM),whichdevelopsandpublishesbestpractices, standards and initiatives in cybersecurity.

The Reserve Bank of India (RBI) has issued a comprehensive Cyber Security Framework for all scheduled commercialbanks(private,foreignandnationalisedbankswhicharelistedintheReserveBankofIndiaAct,1934).Theframeworkrequires allbankstoadheretostrictcybersecurity and data protection guidelines. Generally speaking, the RBI sets the minimumstandardsandnormsfor banks and non-banking finance companies, and other lenders and payment services.

Similarly,theIndianMedicalCouncilissuesguidelinesfortheprotectionandsecurityofhealthandmedicaldataandethicalpracticesbyphysicians and medical services providers and oversees adherence thereto.

2.3 *Securitymeasures*:AreorganisationsrequiredunderApplicableLawstotakemeasurestomonitor,detect,preventormitigate Incidents? If so, please describe what measures are required to be taken.

The IT Act requires all data processors, controllers and handlers to be bound by obligations of transparency, have a lawful basisfortheprocessingofdataandadheretopurposelimitationanddataretentionrequirements.Thelegislationdoesnotprescribespecificmeasures to be taken for monitoring, detection, prevention or mitigation of Incidents.However, the InformationTechnology(ReasonableSecurityPracticesandProceduresandSensitivePersonalDataorInformation)Rulesstatethefollowing insection8:

ReasonableSecurityPracticesandProcedures–

1. A bodycorporateora persononitsbehalfshallbeconsideredto havecompliedwithreasonablesecuritypracticesandprocedures, if they have implemented such security practices and standards and have acomprehensivedocumentedinformationsecurityprogrammeandinformationsecuritypoliciesthatcontainmanagerial,technical,operationalandphysicalsecuritycontrolmeasuresthatarecommensuratewiththeinformationassetsbeingprotectedwith the nature ofbusiness.Inthe eventofan informationsecurity breach, thebody corporateoraperson on its behalf shall be required to demonstrate, as and when called upon to do so by the agencymandatedunder the law, that they have implemented security control measures as per their documentedinformationsecurity programme and information security policies.
2. TheinternationalstandardIS/ISO/IEC27001on“InformationTechnology –SecurityTechniques–InformationSecurityManagementSystem –Requirements”isonesuchstandardreferredtoinsub-rule(1).
3. Any industry association or an entity formed by such an association, whose members are self-regulatingbyfollowingotherthanIS/ISO/IECcodesofbestpracticesfordataprotectionaspersub-rule(1),shallgetitscodesofbestpractices duly approved and notified by the central government for effective implementation.
4. ThebodycorporateorapersononitsbehalfwhohaveimplementedeithertheIS/ISO/IEC27001standardorthecodesofbest practicesfor data protection as approved and notified under sub-rule (3) shall be deemed to havecompliedwith reasonable security practices and procedures provided that such standard or the codes of bestpracticeshave been certified or audited on a regular basis by entities through an independent auditor, dulyapproved bythe central government.The audit of reasonable security practices and procedures shall be carriedout by anauditor at least once a year or as and when the body corporate or a person on its behalf undertakessignificantupgradation of its process and computer resource.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by aregulatoryor other authority, to report information related to Incidents or potential Incidents (including cyber threatinformation,suchasmalwaresignatures,networkvulnerabilitiesandothertechnicalcharacteristicsidentifyingacyberattackorattackmethodology) to a regulatory or other authority in your jurisdiction? If so,please provide details of: (a) the circumstanceinwhichthis reporting obligationis triggered;(b)theregulatoryorotherauthoritytowhichtheinformationisrequiredtobereported;(c)thenatureandscopeofinformationthatis required to be reported; and (d) whether any defences orexemptions exist by which the organisation might preventpublication of that information.

TheInformationTechnology(TheIndianComputerEmergencyResponseTeamandMannerofPerformingFunctionsandDuties)Rules,2013 (the CERT-In Rules) provide for the functioning of CERT-In (see the answer to question 2.6 below).

Rule12oftheCERT-InRulesprescribestheoperationofa24-hourIncidentResponseHelpdesk.Anyindividual,organisationorcorporate entityaffectedbycybersecurityIncidentsmay reporttheIncidenttoCert-In.

TheAnnexuretotheRulesidentifiescertainIncidentsthatshallbemandatorilyreportedtoCert-Inassoonaspossible.Theseareasfollows:

- targetedscanning/probingofcriticalnetworks/systems;
- compromiseofcriticalsystems/information;
- unauthorisedaccessofITsystems/data;
- defacementofwebsiteorintrusionintoawebsiteandunauthorisedchangessuchasinsertingmaliciouscode,linksto external websites, etc.;
- maliciouscodeattackssuchasspreadingviruses/worms/Trojans/botnets/spyware;
- attacksonserverssuchasdatabases,mail,andDNS,andnetworkdevicessuchasrouters;
- identitytheft,spoofingandphishingattacks;
- DoSandDistributedDenialofService(DDoS)attacks;
- attacksoncriticalinfrastructure,SCADAsystemsandwirelessnetworks;and
- attacksonapplicationssuchase-governance,e-commerce,etc.

Rule12alsorequiresserviceproviders,intermediaries,datacentresandbodiescorporatetoreportcybersecurityIncidentstoCERT-Inwithinareasonable time inordertofacilitatetimelyaction.TheCert-Inwebsite provides methods andformatsforreportingcybersecurity Incidents and provides information on vulnerability reporting and Incident response procedures.

Under rule 3(1)(l) of the Information Technology (Guidelines for Intermediaries andDigital Media Ethics Code) Rules, 2021,allintermediariesshallalsoreportcybersecurityIncidentsandsharerelatedinformationwithCERT-InaccordancewiththeCERT-InRules.

2.5 *Reportingtoaffectedindividualsorthirdparties*:AreorganisationsrequiredunderApplicableLaws,orotherwiseexpected by a regulatory or other authority, to report information related to Incidents or potential Incidents to anyaffectedindividuals? Ifso, please provide details of: (a) the circumstance inwhich this reporting obligation istriggered;and (b)the nature and scope of information that is required to be reported.

ThelegislationmandatesonlyreportingIncidentstotherelevantauthorities.TherearenoobligationstovoluntarilyreportIncidents toaffected individuals or third parties.

However,individuals/thirdpartieshavetheabilitytoaccessinformationwithregardtotheirowndataatanytime.Rule5(6)oftheInformation Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)Rulesmandatesthatthebodycorporateoranypersononitsbehalfmustpermitdataprincipalstoreviewanyinformationtheymayhaveprovided to an organisation or body corporate that is processing said data.

The Personal Data Protection Bill 2019, which was tabled in Parliament as of December 2019 but has now been withdrawn bytheGovernment for further amendment, would have broadened the scope of this right for data principals.The Bill provided thedataprincipalwiththeoptiontoobtainfromthedatafiduciaryinaclearandconcisemanner,confirmationofwhetheritspersonaldataisbeing (or has been) processed and a brief summary of processing activities.Arguably, when this information is solicited, the organisationinquestionwouldhavebeenobligatedtoincludeanyinformationwithregardtoanIncidentifitdirectlyaffectstheindividualrequestingthis information.The Bill statedthat the data principal shall also have the right to access in one placetheidentitiesofthedatafiduciarieswithwhomtheirpersonaldatahasbeenshared,alongwiththecategoriesofsuchpersonaldata.

2.6 *Responsibleauthority(ies)*:Pleaseprovidedetailsoftheregulator(s)orauthority(ies)responsiblefortheabove-mentionedrequirements.

Undersection70BoftheITAmendmentAct,theIndianGovernmenthasconstitutedtheIndianComputerEmergencyResponseTeam(CERT-In).CERT-Inisanationalnodalagencyrespondingtocomputer securityIncidentsasandwhenthey occur.TheMinistryofElectronics and Information Technology specifies the functions of the agency as follows:

- collection,analysisanddisseminationofinformationoncybersecurityIncidents;
- forecastandalertsofcybersecurityIncidents;
- emergencymeasuresforhandlingcybersecurityIncidents;
- coordinationofcybersecurityIncidentresponseactivities;and
- issuanceofguidelines,advisories,vulnerabilitynotesandwhitepapersrelatingtoinformationsecuritypractices,procedures, prevention, response to and reporting of cybersecurity Incidents.

The Ministry of Electronics and Information Technology established the Cyber Regulations Appellate Tribunal (CRAT) inOctober2006undersection48(1)oftheITAct.TheITAmendmentActrenamedthetribunaltheCyberAppellateTribunal(CAT).Pursuantto theITAct,any person aggrievedby an order madeby the Controllerof CertifyingAuthoritiesorbyanadjudicatingofficer underthisAct may prefer an appeal before the CAT.The CAT is headed by a chairpersonwho is appointed by the central governmentbynotification, as provided under section 49 of the IT Act 2000.Before the IT Amendment Act, the chairperson was known asthepresidingofficer.Provisionshavebeenmade inthe amendedActfor theCATtocompriseachairpersonandsuchanumberofothermembers as the central government may notify or appoint.

2.7 *Penalties*:Whatarethepenaltiesfornotcomplyingwiththeabove-mentionedrequirements?

Section 70B(7) of the IT Amendment Act states that any service provider, intermediaries, data centres, body corporate orpersonwhofailstoprovidetheinformationcalledfarortocomplywiththedirectionsofCERT-Inundersection70B(6)shallbepunishablewithimprisonmentforuptooneyearorafineofINR 100,000,orboth.However,thisprovision applies only to non-compliancewith specific requests for information by CERT-In under section 70B(6) of the ITAmendmentAct.

Section44(b)ofthe ITAct statesthatifapersonwho isrequiredto furnishinformationunderthis Actorrulesorregulationsmadethereunderfailstodoso,heshallbeliabletoapenaltynotexceedingINR 150,000foreachfailure.Thissectionalso statesthatif apersonwho is requiredto furnish informationfails to do so within a time period specifiedby the Authority, heshall be liable to apenalty not exceeding INR 5,000 for each day of delay until the failure continues.

Section45oftheITActalso provides foraresidualpenalty.Whoevercontravenesanyrulesorregulations under theITAct,forthecontraventionofwhichno specificpenaltyhasbeenprovided,shallbeliableto paycompensationnotexceedingINR 25,000totheaffected party, or a penalty not exceeding INR 25,000.

2.8 *Enforcement*:Pleaseciteanyspecificexamplesofenforcementactiontakenincasesofnon-compliancewiththeabove-mentionedrequirements.

The most recent examples of enforcement are sector-specific.For instance, in July 2021, the RBI recently imposed amonetarypenalty ofINR 50millionon AxisBank,whichisoneofIndia'slargestprivatebanks,for thecontraventionofprovisionsofitscybersecurityframework.Earlierthatsamemonth,theRBIhadimposedapenaltyofINR2.5 milliononPunjab&SindhBank(anationalised bank)forsimilarcontraventions,afterthe bankreported afewcyberIncidents tothe RBI in May.

3. PreventingAttacks

3.1 Areorganisationspermittedtouseanyofthefollowingmeasurestoprotecttheir ITsystemsinyourjurisdiction(including to detect and deflect Incidents on their IT systems)?Beacons(i.e.imperceptible,remotelyhostedgraphicsinsertedintocontenttotriggeracontactwitharemoteserver thatwillreveal the IP address of a computer that is viewing such content)

As indicated at question 2.3 above, all bodies corporate and other data fiduciaries are required to follow reasonablesecuritypracticesandprocedurestoprotecttheirsystems.However,thelegislationdoesnotspecificallyrefertomeasuresthat maybetaken to protect systems against Incidents.

Honeypots(i.e.digitaltrapsdesignedtotrickcyberthreatactorsintotakingactionagainstasyntheticnetwork,therebyallowingan organisationtodetectandcounteractattemptstoattack itsnetwork withoutcausinganydamagetotheorganisation'sreal network or data)

Seetheanswerundertheheading"Beacons"above.

Sinkholes(i.e.measurestore-directmalicioustrafficawayfromanorganisation'sownIPaddressesandservers,commonlyused to prevent DDoS attacks)

Seetheanswerundertheheading"Beacons"above.

3.2 Areorganisationspermittedtomonitororinterceptelectroniccommunicationsontheirnetworks(e.g. emailandinternetusageofemployees)inordertopreventormitigatethe impactofcyberattacks?

Seetheanswersunderquestion3.1above.

3.3 Doesyourjurisdictionrestricttheimportorexportoftechnology(e.g.encryptionsoftwareandhardware)designedtoprevent or mitigate the impact of cyber attacks?

Not specifically.Indian laws do provide for export controls with respect to certain surveillance technologies.Additionally,undertheForeignTrade(DevelopmentandRegulation)ActNo. 22of1992,the DirectorateGeneralofForeignTrade(DGFT)definesitemson the Indian Tariff Classification List and licenses the import and export of theseitems.TheDGFTalso maintainsaseparatelistknownastheSpecialChemicals, Organisms,Materials,EquipmentandTechnologies(SCOMET) List, category 7 of which includeselectronics, computers and information technology, including informationsecurity.However, category 7 does not explicitly defineencryption software and/or hardware.

4. SpecificSectors

4.1 Does market practice with respect to information security vary across different business sectors inyourjurisdiction?Pleaseincludedetailsofanycommondeviationsfromthestrictlegalrequirementsunder ApplicableLaws.

Yes,itdoes.Asthereisnocomprehensivecybersecuritylegislationin India, practicesvarybasedonsector-andindustry-specificnorms,thedetailsof whichare beyond thescopeofthischapter.However,allentitiesmustadheretotheprovisionsoftheITActand various Rules promulgated under the Act, as well as the various other statutes specified in previous answers.

4.2 Excludingtherequirementsoutlinedat2.2inrelationtotheoperationofessentialservicesandcriticalinfrastructure,arethereanyspecificlegalrequirementsinrelationtocybersecurityapplicabletoorganisationsinspecificsectors (e.g. financial services or telecommunications)?

TheRBIprescribesrulesandguidelinesforentitieswithinthefinancialservicessector.TheInsuranceRegulatoryandDevelopmentAuthority prescribessimilarrulesforinsurancecompanies.TheUnified License Agreement requires all telecom companies toreport Incidents to the Department of Telecommunications.Variousother sector-specific rules exist, but a complete discussion ofthese rules is beyond the scope of this chapter.

5. CorporateGovernance

5.1 Inwhatcircumstances,ifany,mightafailurebyacompany(whetherlistedorprivate)toprevent,mitigate,manageorrespond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

TheITActandRules do not explicitlyaddress theissueofbreachofdirectors’or officers’ duties.However,section85oftheITActdoesrequire that inthe eventof contraventionof provisionsof the Act,every person who wasincharge ofand wasresponsibletothecompany fortheconductof itsbusiness(includinga director andany officer)atthetimeofthecontraventionshallbeguiltyofsaid contravention, shall be liable to be proceeded against, and shall bepunishedaccordingly.Theonlyexceptiontothisisifsaidperson(s)canprovethatthecontraventiontookplacewithouttheir knowledge,orthat they exercised due diligence to prevent it.

TheCompanies(ManagementandAdministration)Rules,2014,whichwereframedundertheCompaniesAct,2013,alsorequirethattheboardofacompanyshallappointapersoninthecompanyresponsibleforthemanagement,maintenanceandsecurityofelectronicrecords.Any failure by such person to do so would result in a breach of their duties of care under the law.

5.2 Arecompanies(whetherlistedorprivate)requiredunderApplicableLawsto:(a)designateaCISO(orequivalent);(b)establishawrittenIncidentresponseplanorpolicy;(c)conductperiodiccyberriskassessments,includingforthirdpartyvendors ; and (d) perform penetration tests or vulnerability assessments?

There is no specific requirement for the designation of a Chief Information Security Officer.However, Rule 5(9) of the ITRulesmandatesthatalldiscrepanciesorgrievancesreportedtodatacontrollersmustbeaddressedinatimelymanner.Corporateentitiesmust designate grievance officers for this purpose, and the names and details of said officers must be published on the website ofthebody corporate.The grievanceofficer mustredress respective grievanceswithin a monthfromthe date of receiptof saidgrievances.

TheInformationTechnology(Guidelines forIntermediaries andDigitalMediaEthicsCode) Rules, 2021requiretheappointmentofaGrievanceRedressalOfficerbyallintermediaries,includingsocialmediaintermediaries.TheRulesalsorequirethatgrievanceredressal mechanismsbeavailabletoallusersofsocialmediaintermediariesandbeprominentlypublished.Finally,the Rulesprescribe specific timelines within which relevant action must be taken.

Allremainingobligationsforcompaniesaredescribedinsections2and3above.

5.3 Arecompanies(whetherlistedorprivate)subjecttoanyspecificdisclosure requirements(otherthanthosementionedinsection2)inrelationtocybersecurityrisksorIncidents(e.g.tolistingauthorities,themarketorotherwiseintheir annual reports)?

No,theyarenot.

6. Litigation

6.1 PleaseprovidedetailsofanycivilorotherprivateactionsthatmaybebroughtinrelationtoanyIncidentandtheelements of that action that would need to be met.

Please see the answers in sections 1 and2 above.No specific private remedies are available, but the IT Act and Rulesmakestatutoryremediesavailabletoaffectedpersons.Civilactionsmaybebroughtundersection43oftheITAct,asdiscussedabove.

6.2 PleaseciteanyspecificexamplesofpublishedcivilorotherprivateactionsthathavebeenbroughtinyourjurisdictioninrelationtoIncidents.

AsatAugust2022, noIndiancompanieshavebeenpenalisedfordatabreachessincethedraftingoftheITAct2000.CybersecurityIncidentshavebeenreportedto have impacted52%of allorganisations inIndiaoverthis past year.MajorIncidentsinclude thecompromiseofpassport details of 4.5 million passengers of Air India due to a data breach at the systems of airline data serviceprovider SITA,andtheorder detailsof180millioncustomersofDomino'sPizza.TheCOVID-19testresultsofat least 1,500Indiancitizens also found theirway online due to an attack on a government website.

6.3 Isthereanypotentialliabilityintort(orequivalentlegaltheory)inrelationtofailuretopreventanIncident(e.g.negligence)?

Indiahasrelativelyyoungtort laws,andtheincidenceoflitigationinthis contextis fairlylow.However,intheory, personsaffectedby acybersecurityIncidentandsufferingdamagesdueto non-complianceofabody corporatewithprevailinglawsmay haveanegligenceand/or professional negligence claim against said body corporate.

7. Insurance

7.1 AreorganisationspermittedtotakeoutinsuranceagainstIncidentsinyourjurisdiction?

Yes,theyare.Cybersecurityinsuranceisnotparticularlycommoninthisjurisdiction,butrecentyearshaveseentheconceptpickupinpopularity in certain sectors, including banking and information technology.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such asbusinessinterruption,systemfailures,cyberextortionordigitalassetrestoration?Ifso,arethereanylegallimitsplacedonwhatthe insurance policy can cover?

Thereisnogenerallegislationonthesubject.Regulatorylimitationsoncoverage,ifany,aresector-specific.

8. InvestigatoryandPolicePowers

8.1 Pleaseprovidedetailsofanyinvestigatorypowersoflawenforcementorotherauthoritiesunder ApplicableLawsinyourjur isdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

In additionto the powersofCERT-In discussedin question 2.6 above, the agencymaycall forinformation frombodiescorporate,dataservice providers, intermediariesandsoon,asindicatedinquestion2.7above.TheITActalsoenvisagesaCATinchapterX,whichisnotboundby theIndianCodeofCivilProcedure,1908(CPC)andinsteadisatlibertytoregulateitsownprocedures,limited onlyby the principlesof natural justiceand theITActitself.TheCAThasthe powersofa civilcourt under theCPC and,while trying a suit, such powers shall include:

- summoningandenforcingtheattendanceofanypersonandexaminingthemunderoath;
- requiringthediscoveryandproductionofdocumentsorelectronicrecords;
- requiringevidenceonaffidavits;
- issuingcommissionsfortheexaminationofwitnessesordocuments;
- reviewingitsdecisions;
- dismissinganapplicationfordefaultordecidingit*exparte*;and
- anyothermatterasmaybeprescribed.

Inaddition, section80oftheITActprovidesthepolicewiththediscretiontoenter apublicplaceandsearchandarrestwithoutawarrantanypersonfoundthereinwhoisreasonablysuspectedofhavingcommitted,orofcom mitting,orofbeingabouttocommitanoffence under the IT Act.

8.2 ArethereanyrequirementsunderApplicableLawsfororganisationstoimplementbackdoorsintheirITsystemsforl aw enforcement authorities or to provide law enforcement authorities with encryption keys?

Section 69of the IT Act states that if the Controller of Certifying Authorities is satisfied that it is necessary or expedient to do sointhe interests of: the sovereignty orintegrity ofIndia; the securityoftheState; friendlyrelationswith foreign States; publicorder;orpreventing incitement of the commission of any cognizable offence, for reasons to be recorded in writing, by order, any agencyofthe Government is to be directed to intercept any information transmitted through any computer resource.In such an event,thesubscriberorpersoninchargeofsaidcomputerresourceshall,whencalleduponbytheappropriateagency,extendallfacilitiesand technicalassistancetodecrypt the information.The Act states that any failure to do so will result in imprisonment of up to sevenyears.

AlternativeDisputeResolution:

<u>OnlineADR-AnAvenueforResolvingDisputesinCyberspace</u>

I. TheDevelopmentofADR

Alternative Dispute Resolution (‘ADR’) is evidently not a new phenomenon. Societies have been developing informal and non-adversarialprocessesforcenturiestoresolvedisputes.Asamatter offact, archaeologistshavediscovered evidencethatADRprocesseswere used inancientcivilisationsparticularlyinEgypt,MesopotamiaandAssyria.[1]To-date,oneoftheearliestrecordedmediationsoccurredoverfourthousandyearsagointheancientsocietyofMesopotamia.Itwasdiscoveredthat thethenSumerianrulerusedamediationprocesstohelpavertwar and subsequently developed an agreement in a dispute over land.[2]

TherearemanyexampleswhereADRprocessesweredevelopedintraditionalsocietiesasamechanismtoresolvedisputes.TheBushmenofKalahari, native people of Namibia and Botswana, developed sophisticated systems in order to resolve disputes’ arising thatavoidsphysicalharmandthecourts.WilliamUryheldthat“whenaseriousproblemcomesupeveryonesitsdown –allthemen,allthewomen– andthey talk, andthey talk and they talk. Each person has a chance to have his or her say. It may take two or three days.Thisopen and inclusiveprocesscontinuesuntilthedisputeisliterallytalkedout.”[3]InChina,sincetheWesternZhouDynastyapproximatelytwo thousandyears ago, the post ofa mediator has beenincluded inall governmental administration. Today, it is estimatedthat thereare950,000 mediation committees in China, with at least six million mediators. The said committees handle between ten to twentymillioncases annually,ranging fromfamilydisputestominorproperty disputes.Similarly,inIndiathere hasalsobeenalongtraditionofusingADR as a tool to resolve disputes.The mostadopted and used method of dispute resolution, ‘panchayat’, came into existencesomewhat2500yearsagoandwaswidelyusedtoresolvebothcommercialandnon-commercialdisputes.Inthewesternworld,thedevelopmentofADR can be traced to the ancient Greeks. A public arbitrator position wasintroduced by the city-state around 400 B.C as the Atheniancourts became overcrowded.

Today, ADR is popular in many jurisdictions nolonger as an alternative form of dispute resolution, but rather as a primarymechanism.ADRhasflourishedto thepointwhereithasbeen suggestedthattheadjectiveshouldbedroppedaltogetherandthat‘disputeresolution’shouldbeusedtodescribethemodernrangeofdisputeresolutionmethodsandchoices.[4]Thetwo mostcommonforms of ADR in thiseraconsistofmediationandarbitration.

II. WhatisOnlineADR?

OnlineADRisalsovastlyreferredtoasODR.Itusesalternativedisputeresolutionprocessestoresolveaclaimordispute.ODRisdisputeresolutionthat“takesadvantageoftheInternet,aresourcethatextendswhatwecando,wherewecandoit,andwhenwecandoit.”[5]Itmustbe notedthatODRisnotjustsimplyanonlineversionofADR-rather,theformercomprisesmanyuniqueaspects,fromboth thetechnologicalandprocessperspectives.ODRisrelativelynewintheADRcontinuum,giventhatthefirstarticleonthetopiconlyappearedinlaw journals in 1996. This article will discuss whether ODR is an avenue for resolving disputes in cyberspace.

One of the most insightful writers onODR has commented“in essence,legal disputes resolutionis complexand highly sophisticatedformofinformationmanagementandprocessing.Forthisreason,itlendsitselftotheuseofsophisticatedinformationtechnology.”[6]ODRhas

ADR primarily focuses on moving dispute resolution away from the conventional litigation and court-based decision-making process.Thisprocess is further propagated by designing cyberspaceas the forum to adopt traditional offlineADR processes such as mediationandarbitration.DespiteODRbeing thealternativetooffline methodsofADR,itismuchmorethanjustelectronicADR.ODRisregardedasamulti-disciplinary enterprise which provides secure and confidential dispute resolution processes. Commercial online disputeresolutionserviceshavebeenofferedsince1999,withmostODRfacilitatorsbeingbasedintheUnitedStates. Overtheyears,ODRprovidersgloballyhavesteadilyincreased.

In January 2000, for the first time, parties located in the four corners of the globe successfully resolved international legaldisputescompletely online. There were no meetings between the parties, but there was an exchange of documents, comments andevidence,which were produced underthe vigilanteye of an appointedarbitratorslocated ina differentcountry.This dispute– concerningdomainnames - was arbitrated under the dispute resolution policy and rules of the Internet Corporation for Assigned Names andNumbers(ICANN),andwasadministeredbyeResolution -theprimaryorganisationprovidingacompleteonlineresolutionservice relatingtodomainnamedisputes.Today,theusageofInternetasarevenuetoresolveaparticulardisputeisbecomingmainstream,althoughitstillraises afew questions.

III. TheInternet

Previously,thetechnicalskillsandexperiencerequiredtooperateacomputercommunicationssoftwareorequipmentwasfarbeyondthecapabilitiesofanon-specialist.However,inthepresentday,evenextremelysophisticatedandadvancedinformationtechnologyiseasilyaccessibleto non-specialist users. The Internet itself is a global connection of interconnected computer networks, and the World WideWeb was designedspecificallytofacilitatethesociety’saccessibilitytoinformation.

The growth of Internet has been exponential.As early as 1994, it was estimated that therewere15 million users online,approximatelybelowonepercentoftheglobalpopulation.Presently,thereareapproximately3.5billionusersonlineaccountingforoverfortypercentofthe global population.[7]

The leading factor causing the development of ODRis e-commerce, covering both elements - business-to-business (B2B) and business-to-consumer(B2C).TheCensusBureauoftheDepartmentofCommerceoftheUnitedStatesinNovember2016releasedthattheestimateoftheUnitedStates retail e-commerce sales for the third quarter of 2016 itself sums up to$101.3 billion.[8]Due to this largeamount of transactions,e-commercerequiresaneffectiveandefficientsystemofdisputeresolutionthatallowsatradertomaintainconsumerconfidence,as the traditional institutions that create trust are absent.

IV. OnlineMediation

OnlinemediationisthemostfrequentlyusedmechanismofODRforthesimplereasonoftherebeingfew,ifany,legalorprocess restrictionsonmediation.Most,ifnotall,ODRprovidersoffermediationforanydisputethatisperceivedas‘amenabletomediation’.Thiscoverstheentirespectrumofe-commercedisputestoemployment,insurancedisputesandpersonalinjurymatters.

The mode of communications used in an ODR includes e-mail, fax, telephone, and of course web-based communication such aschat,instantmessaging,onlineconferencing, web-postingandvideoconferencing.Thefactthattherehasbeenasignificantincreaseinthequalityofvideotechnologyover therecentyearscombinedwith theadvancementinInternetspeedwilldirectly amounttothe growthandimportance of ODR.

A mediation process, whether conducted online or offline, is a confidential process on a non-prejudicial basis. These conditionsarerequired as pre-requisites in order to facilitate open communication and disclosure of information by parties to achieve asustainableresolution covering each party’s needs andinterest. However, it is crucial totake into account that the protection ofelectroniccommunicationsfromanyformofaccidentaldisclosureisnotcoveredbygeneralstatementsspecifyingconfidentiality.Further,aspecific policy on this crucial issue is also absent on almost all ODR provider websites.

V. OnlineArbitration

Onlinearbitrationis availableforallsorts ofdisputes whetherarisingonlineoroffline.Itis mostcommonly utilisedindisputes arisingfromcommercial matters and online activity. Over fifty percent of ODR providers offer online arbitration as an available service. Further,theAmericanArbitrationSociety(AAA)providesforarbitrationservicesundervariousinstitutionalrulesanditssupplementaryproceduresfor online arbitration permits for arbitration processes to be conducted online.As of 2006, 3,000 out of 160,000 arbitrationcaseswhichwere handled by AAA were conducted on a digital basis.[9]This shows that there is acceptance to online arbitration by society and the numbersaregrowingonarapidscale.Thisisasignificantfactillustratingthatonlinearbitrationmaintainsthelevelofformalityrequired.

Additionally, theADRInstitute of Canada National Arbitration Rules provides that an arbitration bymeans of electroniccommunication,andapartorallofthearbitrationmaybeconductedbytelephone,e-mail,Internet,oranyotherelectroniccommunicationifthepartiesagree.[10]AnexpressprovisionintherulesoftheWorldIntellectual Property Organisation (WIPO) Arbitration and Mediation Centre – whooffersarbitrationandmediationfocusingonintellectualpropertyandcommercialdisputes,includingdomainnamedisputes– allowsforpartiestooptforan onlineprocess.Tothecontrary,theInternationalChamber ofCommerceInternationalCourtofArbitrationsituatedinParis and theLondon Court of International Arbitration providearbitration services but do not at the moment have specificODR rules.
Similarly,theHongKong International ArbitrationCentreoffersinternationalarbitrationanditsrulesgoverning electronictransactionspermits for the resolution of e-commerce disputes.

VI. AdvantagesofOnlineADR

SimilartoofflineADR,onlineADRallows theneutraltofirstadapttheprocesstoaddresstheparticularneeds of thedisputants.[11]Additionally,therearealsoadvantagestoresolvingdisputesovertheInternet.“Theprocesswillallowforgreater flexibility,morecreativesolutionsandquickerdecisions”.[12]

Traditional ADRand cyber ADR both providesubstantial savingswhencompared to litigation, which isextremely costly. Asa matteroffact,ODRisa morefeasibleoptionincomparisontoofflineADRfordisputantswhoareunabletoaffordtravellinglong distanceorforthoseinvolvedine-commercedisputesforlowmonetaryvalue.[13]Moreoftenthannot,onlinedisputesarisebetweenindividualsfrom greatdistances,whereatleastonepartywillberequiredto travelthedistanceiftheofflinemodeofADRisreliedupon. Therefore,withtheexistence of ODR, parties can now participate in an ADR process from their respective preferred location and thissimultaneouslyreduces costandtravellingtime.Thereisalso noneedforthepartiestoincuradditionalcost for therentcharges inbooking a neutralfacility in order to conduct the respective ADR process.

There are also significant benefits that stem from the very nature of e-mail mode of communications. E-mails, listservs and webpostingscan be written, responded and posted at any time making online mediation much more convenient. The traditional mediationprocessrequiresschedulingwherebyitisabsolutelynecessarytoarrangethetimeandvenueforameetingandfrequently,thisrequirementposessomedifficulties.Onthecontrary,online mediationallowsfortheparties toparticipateinthemediationprocesswhenthey areavailableandat convenient times.[14]

Another crucial advantage of online mediation is that the amount of idle time that the disputants experience is significantlyreducedbecause unlike conventional mediation,the mediator can devote time to one partywithout wasting thetime of the other party,whowouldotherwisesitaroundwaitingforthenextmediationstage.AsJimMelamedstated,“Experiencedmediatorsarewellawareofthebenefits of asynchrony. This is a big part of the reason many mediators ‘caucus’ with participants. Mediators want toslow the processdownandassistparticipantsincraftingmorecapablecontributions.Thisconceptofslowingtheprocessdownandallowingparticipantstosafelycraftheir contributions is at the heart of caucusing. Surely, the Internet works capably as an extension of individual party caucusandisremarkablyconvenientandaffordable.Internetcommunicationstakelesstimetoreadandclientsdonot hearthe professionalfeemeter clicking.WhentheInternetisutilisedforcaucus,the‘non-caucusingparticipant’doesnotneedtositinthewaitingroomorlibraryreading *Time*magazineorgrowingresentful atbeing ignored.[15]

Itmayalsobearguedthatmorethoughtful,well-craftedcontributionsare adirectresultoftheabilityofthepartiesto editmessagespriorto sendingthem.Also,many online mediationmechanismsareavailableallday,everydayoftheyear.Therefore,disputantscanproceedtonegotiateand commence their mediation process immediately.

It is alsoimportant to note that participants in theODR process can access expertise that would not otherwise beavailablelocally,whichhas a direct potential benefit for the people in areas where skilled or specialised disputeresolution assistanceis not available orlimited.Further,ODRminimisesjurisdictionalissuesandalsoworksasagoodtoolforsecuritywhereonepartywantstokeeptheirlocationsecret;fo rexample, where there is a record of domestic violence between the parties.

VII. ChallengesinOnlineADR

Whilstusingcyberspaceasaplatformtoresolvedisputeshasmanyadvantages,i.e.fasterandcheaperresolution,therearetypicallyanumberofdrawbacks that need to be considered.

Dueto the borderless nature of the Internet, online ADR faces issues concerning enforcement; enforcing the agreement to conductanADR proceeding and enforcement of the actual award. Whena contract is entered into between the parties online, it is createdinanelectronic form.Theissuearisingfrom thatfactis thatinmanyjurisdictions,aswellasontheinternational plane,ADRagreementsmustbe inwritinginorderforittoberecognised.IntheUnitedStates,theFederalArbitrationActandtheNewYorkConventionontheRecognitionand Enforcement of Foreign Arbitral Awards of 1958 requires agreements to be inwriting. That clearly implies that for anypersonlivingin the United States, an ADR agreement included in an electronic format may not be recognised. However, it has beensuggestedthattheterm'inwriting'shouldbeinterpretedtoincludeelectronicagreements.Nonetheless,therehasbeennodecisionto-dateon that matter, thus leaving such agreements as void.

Even if thematter aboveis met anda decision is achieved, that particular decision will then need to be enforced bya particular state.Theissue here is the choice of law to be adopted. Naturally, theagreement itself may provide a provision expressing thechoice of lawrule.Despitethat fact, rules for discovery and evidence differ greatly between jurisdictions and procedural differences might also beanissue.Moreimportantly,thekeyelementtobenotedisthataparticularstatemayrefusetoenforceanyawardsobtainedinajurisdictionwhichhasprocedures which are in conflict with the particular state legal framework.

Additionally, among the ever-present issues in the cyber world is security. Safe and reliable communication between counsel andclient,betweenthecourtandaparty,oreveninbetween thepartiesisabsolutelyrequiredfor onlineADRtowork.Security ofcommunicationisamajor concern in thecyber world. Taking into account thefact that new encryption technologies are constantly created andupdated,every encryption can eventually be broken. One such technique where unauthorized access is commonly gained is 'spoofing'where theunauthorized personassumes theidentity ofan existing authorized user toaccess confidential information.Snifferpackagesareeasilyavailableonlineandmay beusedtointerceptand manipulateparticulardata.Amoresecured mechanismwouldbetheuseofclosedsystems, which are screened from the Internet. In other words, close systems used dedicated private lines to transmitcommunications.Therefore,itisarguablethattheinternetposes higherlevelofthreats toconfidentialinformationwhencomparedtoaface-to-facecommunication during a conventional ADR process.

AnotherchallengefacedbyonlineADRistheelementoftrustontheverybasisthatinallhumanrelationswhethercommercialorprivate,trustplaysan important role. Therefore, one does not know the personalities of the neutrals or worse, what to expect from the provider.If theparties decide to proceed nonetheless, thelack of trust betweenthe partiesmight causea negative atmosphere, causing lesswillingnessto compromise on the disputed matter.

ConventionalADRinvolvesatriangle,i.e.thepartiesandthepresenceofaneutral.[16]TheonlineADRprocessintroducesafourthparty, whichisthetechnologythatworkswiththeneutral.Thefourthpartydoesnotreplacetheexistenceorpositionoftheneutralanditisnot ofcoequalinfluence,butratherfunctionsasanally,collaboratorandpartner.[17]Inotherwords,thefourthpartyisessentiallyamore sophisticated version of a penand pencil.Appropriate use of technology in the present day of changes is critical to any successfulODRprocess.Oneofthebiggestchallengesinbuildingandrunninganonlinedisputeresolutionprocessistobalanceandintegratethehuma nandtheautomated dimensions of the cyber world.

VIII. BestPractices

SmartlydesignedonlineADRsystemscanenablesuperioroutcomes,muchhigherqualityservices,andgreaterengagementbetweentheneutralandt hedisputants.AnADRprocesswillnotbeused,orbesuccessful,until andunlessitiscapableoffacilitatingaccess andparticipation,and mor e importantly offers value to its users.[18]Online ADR initiatives were derived from governments, industry, consumer associations and dispute resolution providers. Suggested best practices of ODR have been developed by variousgroupsincludingtheAmericanBarAssociationTaskForceonEcommerceandADR[19],ConsumersInternational,theNationalAlternativeDispute ResolutionAdvisoryCouncil(Australia),andtheWorkingGrouponElectronicCommerceandConsumers(Canada).[20]

Best practices of ODR suggested by these groups include; independence, transparency, availability, affordability, effectivenessandvoluntaryparticipation.Someguidelinesfurthersuggestedthat,“Whileformaltrainingisnotrequired,they[theserviceproviders]s houldbefamiliar with basic legal concepts.”[21]Additionally, guidelines also suggested that an online dispute resolution system shall also includeensuringthenecessarylevelofsecurity,andstoringinformationonlyforsolongasitisrequiredinordertoachievethepurposeforwhichitwa s collected. The destruction of data shall be irreversible.

IX. OnlineADREffectiveness

Atpresent,therearemillionsofonlinetransactionsandasadirectresulttherearesignificantnumberofdisputes.Annuallymillionsofcases arehandled across eBay and PayPal platforms in more than16 different languages which clearly indicates the need for anonlinedisputeavenue.

Many arein the view that online ADR makes most sensetypically incases where legal costs would exceedwhat could berecovered.However,manylargeorganisations,particularlyinsurancecompanies,findthatonlineADRsavesthemmoneyeveninbig-moneycasesonthebasisthatcasescanbe handledata muchfasterspeed.Asanexample,Cybersettle,anonlinedisputeserviceprovider,focuseson online insurance claims. Cybersettle states that it “…expedites settlement by eliminating egos and posturing. Both sides get to thebottomlinequicklyand confidentially,knowingthattheir figureswillnotberevealedtotheopposition.EvenifpartiesdonotsettleonlinethroughCybersettle,thedisputecansettleshortlythereafterthrought raditionalnegotiations, or with the assistance of our telephone facilitators becauseCybersettlemovespartiesclosertoresolution.”[22]

Despiteitsdifficultytoobtain publishedstatementratesforonlineADRareverymuchcomparabletotheconventionalADRstatementrates ranginginbetween60percentto85percent.[23]OnestudyinrelationtotheeffectivenessofonlineADR particularlymediation conductedin2001,opinedthat“…withacommitmenttoprocess,properorganisationandanexperiencedmediator,neitherthenatureofthedispute nor its characteristics would change the potential of the online process to achieve a final and mutually acceptablesolutionwherethatisthegoaloftheprocess.”[24].

OnlineDisputeResolution(ODR):

OnlineDisputeResolutionistheresolutionofdisputes,particularlysmallandmedium-valuecases,usingdigitaltechnologyandtechniquesofAlternate Dispute Resolution(ADR), such as negotiation, mediation, and arbitration.

Whyisitinnews?

InJune2020,NITIAayog,inassociationwithAgamiandOmidyarNetworkIndia,broughttogetherkeystakeholdersinavirtualmeeting foradvancingOnlineDisputeResolution(ODR)inIndia.SeniorjudgesoftheSupremeCourt,secretariesfromkeygovernmentministries,leadersofthe industry, legal experts and general counsels of leading enterprises participated in it.

ConsideringtheongoingCOVID-19pandemic,onApril10,2021,ahandbookonODR,developedbyAgamiandOmidyarIndia,in associationwithNITIAayogandwiththesupportofICICIBank,AshokaInnovatorsforthePublic,Trilegal,Dalberg,DvaraandNIPFPwasreleased.

ThisisanimportanttopicfromtheperspectiveoftheupcomingIASExamandquestionsbasedonthesamemaybeaskedintheprelims examination.Candidatescanrefertothebackground,origin,objectivesandimpactofODR.

OnlineDisputeResolution(ODR)–Origin&Background

TheoriginsofODRcanbetracedtotheevolutionoftheInternetinthe1990s,whichincreasedonlinetransactions,andtherebydisputesrelatedtosuchtransactions.

Broadly,ODR’sdevelopmentacrosstheworldcanbedividedintothreephases,witheachphasebenefitingfromthesubsequent innovationsinInformation Communication and Technology(ICT). Discussed below are the three phases:

- **FirstPhase:eBay’sexperimentleadstheway**
  - Thefirst initiativeson ODRprojectswerelaunchedin1996intheUniversityofMassachusettsandtheUniversityofMaryland
  - Withthedevelopmentofe-commerce,arobustsystemwasrequiredforoperatingcommercialactivitiesontheinternet. ODRofferedasolutiontothis problem
  - In1999,eBaystartedapilotprojecttoprovideonlinemediationfacilitiesfordisputesarisingbetweenbuyersandsellersonitsplatform
  - By2010eBaywashandlingoversixtymilliondisputesperyearthroughitsODRplatform
- **SecondPhase:BoomofODRstart-ups**
  - Thesuccessofthismodelandtherapidgrowthoftheinternetkick-startedtheevolutionofODRandledtotheboomofODRplatforms. There were up to 21 new ODR programs that were launched in the year 1999
  - OnlyafewsuccessfulplatformssuchasCybersettle,SmartsettleandtheMediationRoomwereabletomakearemarkableimpactinthedisputeresolutionecosystem
- **ThirdPhase:AdoptionbytheGovernmentandJudiciary**
  - ThesuccessofafewoftheprivateODRplatformsdrewtheinterestofgovernmentstowardsthisemergingadditiontothe dispute resolution ecosystem

OnlineDisputeResolutioninIndia

The United Nations Commission on International Trade Law (UNCITRAL) adopted the UNCITRAL Model Law onInternationalCommercialArbitrationin1985andtheUNCITRALConciliationRulesin1980.Inthecontextofinternationalcommercialrelations,this Model Law has been recommended by the United Nations General Assembly(UNGA).

IndiaincorporatedtheseuniformprinciplesofADRintheArbitrationandConciliationAct,1996.

InthecontextofIndia,givenbelowisthetimelineforODRdevelopmentinIndia:

2006	NationalInternetExchangeofIndiaadopted‘.IN’domainnameDisputeResolutionPolicy(INDRP)whichprovidedtheODR
2011	Chennaihostedthe10thAnnualInternationalForumonODR
2017	MinistryofLawandJusticeissuedastatementtourgeGovernmentagenciestoresolvedisputesthroughonlinearbitration
2018	MinistryofMSMElaunchedSAMADHAANPortaltoaddressdelaysofpaymentdisputesinvolvingMicroandSmallenterprises
2019	E-ADRChallengewaslaunchedtoidentifyandsupportODRstart-ups
2020	• ThegovernmentofIndialaunchedtheVivaadseVishwasSchemefortheefficientresolutionoftaxdisputesthroughODR • VidhiCentreforLegalPolicypublishedareportonmainstreamingODRinIndia • NITIAayogestablishedacommitteeundertheChairmanshipofJustice(Retd.)A.K.Sikritobroad-basetheuseofODRinIndia • ChhatisgarhconductedthefirstvirtualLokAdalatandprovidedconciliationservices • Department-relatedParliamentaryStandingCommitteeonPersonnel,PublicGrievances,LawandJustice,intheirreportcalledfortintroduction oftechnology in the arbitration and conciliation process

ODRinIndia&COVID-19

DuringtheongoingCovid-19pandemic,thetargetistolookintoCovid-relateddisputes(mostnotablyinlending,credit,property,commerceandretail) through ODR, which is an important part of the economic revival.

Itwillsetintomotiontheuseoftechnologytowardsefficientandaffordableaccesstojustice,especiallyinpost-pandemictimes.

Also,readCoronavirus&DigitalSolutions:RSTV-BigPicture

BenefitsofODR

- **Cost-Effective–** ODRhasthepotentialtoreducelegalcosts.First,bywayofreducedtimeforresolutionandsecond,bydoingawaywiththe need for legal advice in the select category of cases
- **Convenientandquickdisputeresolution**–ODReliminatestheneedfortravelandsynchronisationofschedules
- **Increasedaccesstojustice**– AspartofIndia’scommitmentandleadershiptoattainSustainableDevelopmentGoalsadoptedbytheUNGeneralAssemblyin 2015,Indiaiscommittedtoensuringequalaccesstojusticeforall. SinceODRtools suchas online

negotiationandmediationarepremisedonmutuallyarrivingatanagreement,theymakethedisputeresolutionprocesslessadversariala nd complicated for the parties

- **Removesunconsciousbias**–ODRprocesseslessentheunconsciousbiasoftheneutralwhileresolvingdisputes
- ExploringthemassivepotentialofOnlineDisputeResolution(ODR)can**enhancethe**EaseofDoingBusinessinIndia.

CurrentStatusofDisputeResolution

- AlthoughwehaveobservedariseintherankingofEaseofDoingBusiness,wehavealotmoreroomtocoverinEnforcingContracts.
- Weareranked163rdincontractenforcementwhichisamarginalimprovementfromthe186thrankin2015and173rdin2016.
- Wealsofarepoorlyintimetaken(4yrs)andcost(morethan30%ofprojectcost)fortheseobligations.
- Wehavealsoacquiredareputationforbeingarbitration-unfriendlyaspertheSrikrishnaCommittee(2017)report.

AdvantageofTechnologyinODR

- Itreducestheburdenonthecourtsandsavestime.
- Itiscost-effectiveandprovideseffectiveresolutions.
- Usingadvancedtechnologysuchasblockchain,naturallanguageprocessing,artificialintelligence,andmachinelearningwill bea gamechanger in the coming years.
- CorporatesandprivateplayersarealreadyusingODRtoresolvedisputesinlakhsofvalue.
- Govt.institutionssuchastheNPCI,andtheReserveBankofIndiahaveledthewaybyincorporatingODRmechanismsintoseveralof their initiatives.

ChallengesofODR

- **Digitalliteracy–** ODRrequiresabasiclevelofdigitalliteracyasaprerequisite.InIndia,digitalliteracyoftenvariesacrossage,ethnicityand geography. This digital divide needs to be addressed to ensurethat ODR isadopted by societyat largeand notremainlimited to urban areas
- **Digitalinfrastructure**–AbroadbaseadoptionofODRwillrequireessentialtechnologyinfrastructureacrossthecountry
- **LackoftrustinODRservices–** Alotofpeopleinthecountrydonottrusttheemergingtechnologywhichisamajorchallengeforthepeople of India
- **Privacyandconfidentialityconcerns** –Greaterintegrationoftechnologyandreducedface-to-faceinteractionscreatenewchallengesforprivacyandconfidentiality,especiallyindisputeresolution

Examplesfromaroundtheworld

- AsmallcountrylikeSingapore,starteditsSingaporeInternationalArbitrationCentreinthe1990swhenIndiawasopeningupforforeigninvestment.
- Sincethen,ithasemergedasaglobalarbitrationhubwhichisexemplifiedbyitstopspotin'EnforcingContracts'.
- Ironically,Indiancompaniesareamongitstopclients.

WayForward: Although the amendmentsalong with judicial decisionsinrecent years have put India ontheright path, we needtoincentivisetheuseofODRasadefault disputeresolutiontool. Withrisingonlinetransactions, fast-trackingenforcement ofODR istheneedofthehour. AsNITI AayogclaimsthatIndiaisuniquelypositionedtoemergeasthe epicentrefor thedevelopmentsinODR, weneedtosolvetheissues of funding, infrastructure and public policy support to make it happen.

UPSCaspirantscanalsoreadaboutthein-depthRSTV–BigPicturediscussionsaboutCoronavirus&ImpactontheEconomyatthelinked article.

OnlineDisputeResolution(ODR)[UPSCNotes]:-

FrequentlyAskedQuestionsaboutOnlineDisputeResolution

Q1

WhatisCourt-RelatedOnlineDisputeResolution?

Court-relatedOnlineDisputeResolution(ODR)isapublicfacingdigitalspaceinwhichpartiescanconvenetoresolvetheirdisputeorcase.

Threeessentialcomponentsdifferentiatecourt-relatedODRfromotherformsoftechnology-supporteddisputeresolutionQ2

Whatisthepurposeofonlinedisputeresolution?

TheprimarypurposeofODRistoallowthepartiestoresolvetheirdisputewiththeuseofelectronictechnology.Itmayoccurin“realtime”orunrollinan asynchronous manner, depending on the rules ofthe ODR Provider, as well as the wishes ofthe parties.

GetfamiliarwiththeUPSCSyllabusfortheprelimsandmainsexaminationfortheupcomingCivilServicesExamatthelinkedarticle.

Forthelatestexamupdates,studymaterialandpreparationtips,candidatescanturntoBYJU’Sforassistance.

UNIT-4

ElectronicBusinessandlegalissues:
EvolutionanddevelopmentinE-commerce: Inthisarticle,you'llexploretheevolutionofhackingandcybersecurity.ShareWhenENIAC,thefirstmoderncomputer,wasbroughtonlinein1945,**cybersecurity**wasn'tawordyoucouldfindinthe dictionary. The only way to interact with the building-sized computers of the era was to be physically present, so virtual threats weren't a risk, and access control was a matter of physical security.

Cybersecurity developedasa distinctfieldthroughoutthe1960sand70sandexplodedintothepublicconsciousnessin thelate1980s, aftera series ofevents that highlightedjust how dangerous a lack of security could be. Continuingtogrow throughout the90s, cybersecurity is now a core part of modern life. Let's explore the brief history of this field!

Origins

Whenyouheartheword**"hacker"**,youprobablythinkofamysteriousindividualsittingaloneinadarkroom,watchinginformationscroll by on multiple windows as they conduct nefarious deeds.

Themediaoftentakescreativelibertieswhendepictinghackers.Itmaysurpriseyoutolearnthattheoriginofthe'modernhacker' wasacountercultureofpeopletinkeringwithtechnologyorfindingnewwaysofsharinginformation.Hackingisnotinnatelytied tobreakingintocomputers.Infact,anearlyinstanceofhackingin1963involvedhackingaphonesystemtomakelong-distance callsforfree.Hackingistheactofworkingwithintheconfinesofasystemtoproduceunintendedbehavior.Thatbehaviorranges from cracking passwords to saving a spaceship's air system using spare parts.

The1960's

The more connectedwe are,themore important cybersecurityis, andthe widespreadadoption of time-sharinginthe 60swasa big increase in connectivity. Computers of the era were expensive and bulky; timesharing let multiple people use a single large computer at the same time, which meant that precautions were needed to prevent unauthorized access to files and to the computeritself. Computingtimewasexpensive in those days! The solution of protectingaccountswith passwords haspersisted to modern times.

The1970's

ThecreationofARPANET,theearliestformoftheinternet,gavehackersalottothinkaboutandexplore.ARPANETwasatesting ground for new technologies, and the hacker and technical communities busied themselves with developing and prototyping newtechnologies,includingemail.Therewerea fewadventuresinto thedevelopmentofmalware(shortformalicioussoftware),including Creeper and Reaper, the first computer worms, but these were academic exercises more than anything else.

I'MTHECREEPER:CATCHMEIFYOUCAN
ThemessageyouwouldhaveseenifyoureceivedavisitfromCreeper!

In this era of rapid development and experimentation, the security of the technology being developed was not a concern. The widespreadviewofARPANETasacooperativeacademicendeavorandtheabsenceofwell-establishedbestpracticesmeantthat the motivation and means to design secure systems and software were limited. However, people were starting to think about security. A 1975 paper titled*The Protection of Information in Computer Systems*presented principles and concepts that would become critical to cybersecurity in the future.

The1980's

The1980swereachaotictime;theInternetwasformedin1983,andtheadoptionoftheInternetProtocolSuitebyARPANETand other networks added more potential targets and attackers to the mix. The first "real" malware emerged during this time, as did the public panic around The Cold War. Tools and techniques developed during this era would become common in modern cybersecurity; dictionary attacks used stolen lists of passwords and exploited weak default credentials, while decoy computer systems trapped attackers.

Thelate80'sgavetwomajorevents.

- ThefirstwasthediscoverythatahackerworkingfortheKGBgainedaccesstosensitivedocumentsfromtheU.S.military.

- Thesecondwasthecreationoftheworld'strulyseriouspieceofmalware:the MorrisWorm.Itwasoriginallywrittento map the sizeoftheinternet but quickly grew out ofcontrol,chokingcomputerswith multiple copies ofitself, andcloggingthe network as it kept replicating.

Theseincidencesexploitedunsecureddefaultsettings;defaultpasswordslike"admin"ensuredasystemorpieceofsoftwarewas easilyexploitable.

The1990's

The 1990s are widely considered to be the era of viruses. Computers that connected to the internet became more common in householdsandthisincreased access. Thisled to unskilled *script kiddies*— individuals who download a piece of code andrun it withouthavingtowriteanycodethemselves.Theycanusethatcodetolaunchattackstheydon'tunderstandinordertovandalizeordestroy targets for fun.

Theunfocused,scatteredattacksoftheeraledtotheriseoftheanti-malwareindustry,evolvingfromacuriositytoacorepartof moderncybersecurity.Cybersecurity,asawhole,startedtobetakenmuchmoreseriously.Largecompaniesmadepublicpushes to improvethesecurityoftheirproducts.Householdcomputerswereoftentargetedbytherampantmalwareoftheera, demonstrating the consequences of poor cybersecurity to their owners.

The2000's

Moreandmoredatabecamedigitized—particularlymonetarytransactions.Asthescriptkiddiesofthe90sgrewupandgained more experience, the scale of threats shifted, and attackers started having larger targets beyond vandalism and destruction. Credit-card breaches, hacktivism, and holding corporations' systems for ransom became increasingly common, as malicious hackers realized there was real money to be made from cybercrime.

Hundredsofmillionsofsetsofcreditcarddatawerebreachedoverthecourseofthedecade.

The threats of data breaches and ransomware attacks forced large businesses to improve their cybersecurity programs. Being hackedwasnolongerjustamatterofvandalism;itcouldleadtoextendeddowntime,lossofcustomerloyalty,lawsuits,andfines from regulatory bodies.

The2010's

During the 2010s, the scale of threats continued to grow: Attacks by nation-states increased in frequency, and they carried out infiltration and surveillance campaigns and deployed cyberweapons to attack strategic objectives. Malicious hacker groups targeted major corporations and government organizations, stealing data and launching ransomware attacks, and the growing number of smart devices in circulation gave these groups an entirely new type of target.

The most dangerousofthese newthreat actorsare known asAPTs: AdvancedPersistentThreats. Oftenfundedbynation-states, APTspossessresourcesanddeterminationfarbeyondwhatsmallerthreatactorsmighthaveaccessto.Whilelesser threatactors mightbecapableoflaunchingcyberattacksagainstatarget,APTsarecapableofrunningentirecyber-campaigns,attemptingto infiltrate their target across multiple domains simultaneously.

Large-scale cybersecurity incidents became more and more common: WannaCryandNotPetyacaused global damage, the [Equifax) andYahoo!breaches revealed hundreds of millions of pieces of personal information, and countless companies and organizations were hit by ransomware attacks, bringing their operations grinding to a halt.

Thepresent

Withtheworldasconnectedasitis,cybersecurityisaboutprotectingpeopleasmuchasitisaboutprotectingcomputers.People arefallible,and,likecomputers,wehavevulnerabilitiesthatcanbeexploited:Emotionalmanipulationandsocialengineeringarepowerful tools, used by hackers to gain access to secure systems. Many of the systems we rely on run on computers, and the stakes for protecting them have never been higher. Attacks on those computers can disrupt transportation, power, economy, healthcare, communication, and even lives.

With computers so integratedinto our lives, it's crucial that we protect them. In cybersecurity, we mustlearn from our mistakes, applying the lessons learned in the past to prevent attacks in the future. This is the domain of security researchers and ethical hackers:Finding and fixing vulnerabilities beforethey canbeexploited,and helping to makeus and our computers as safeas possible.

GrowingAspectsofCyberSecurityinE-Commerce:

The world is witnessing a transition from in-storeshopping to onlineshopping. E-commerce (Electronic commerce) giants such as Amazon, Alibaba, eBay etc. are leading the way towards this change. Much technological advancement are being made to ease the life of mankind with online shopping being the most notable. E-commerce is known to be a powerful instrument for transformationofbusinessthatgivescompaniestheopportunitytoupgradetheirsupplychainoperations,improvetheirnetwork, as well as provide better services to both customers and suppliers. Applying the techniques of online shopping that yield such advantages may not be possible without the presence of a well-organized approach to E-commerce security. E-commerce organizationssuchasAmazonandAlibabahavealsobeenusingsuchtechniquestoensuredataprotection.Themostcommonofthemall is the One Time Password (OTP), which is sent to a user when they make payments online for identity verification. Ontheotherhand,AlibabausesauniqueKeyManagementSystem(KSM)whichisafullymanagedservicethathelpscustomers create, delete, andmanageencryption keys toprotect data. This system provides availability, reliability and elasticity alongsidesecurity and compliance. The paper also explore the importance of different security algorithms in Ecommerce domain.

papervspaperlesscontractsE-Commercemodels-B2BandB2C:

HowdoB2CandB2Be-commercecontractsaffectyourliability?

If you run an online business, you needto understandhow different types of e-commerce contracts affect your liability. Whetheryou sell toconsumersorotherbusinesses,yourcontractscanprotectyoufromlegal disputes,orexposeyouto unwantedrisks.Inthisarticle,wewillexplainthemaindifferencesbetweenB2CandB2Be-commercecontracts,andhowtocreate effective and enforceable agreements for your online transactions.

WhatareB2CandB2Be-commercecontracts?

B2CandB2Bareabbreviationsforbusiness-to-consumerandbusiness-to-businesse-commerce.B2Ce-commercerefersto onlinetransactionswhereabusinesssellsgoodsorservicesdirectlytoindividualconsumers.B2Be-commercereferstoonline transactions wherea business sells goods orservices toanotherbusiness.B2CandB2B e-commercecontracts are thelegal agreements that govern these transactions. They can be written, oral, or implied by the conduct of the parties.

WhyareB2CandB2Be-commercecontractsimportant?

B2C and B2B e-commerce contracts are important because they define the rights and obligations of the parties, and the remediesincaseofbreach.Theyalsoaffecttheliabilityofthepartiesforanydamages,losses,orclaimsthatmayarisefromthe onlinetransactions.Forexample,aB2Ce-commercecontractmayincludetermssuchasdelivery,warranty,refund,privacy,anddispute resolution. A B2B e-commerce contractmay include terms such as payment, delivery, quality, intellectual property, and indemnification.

HowdoB2CandB2Be-commercecontractsdiffer?

B2C and B2B e-commerce contracts differ in several ways. First, B2C e-commerce contracts are subject to more consumer protection laws and regulations than B2B e-commerce contracts. These laws and regulations aim to protect consumers from unfair, deceptive, or abusive practices by businesses. For example, a B2C e-commerce contract must comply with the Federal TradeCommissionAct,theElectronicSignaturesinGlobalandNationalCommerceAct,andtheConsumerReviewFairnessActintheUS. A B2B e-commerce contract may not be subject to these laws and regulations, or may have more flexibility to negotiate the terms.

Second,B2CandB2B e-commercecontractshave differentlevels of complexityandcustomization.B2Ce-commercecontracts are usually standardized and simple, as they are designed for mass-market transactions. They often use clickwrap or browsewrapmethods to obtain the consent of theconsumers.These methodsinvolveclickinga button orbrowsinga website to indicate acceptance of the terms and conditions. B2B e-commerce contracts are usually more complex and customized, as theyaredesignedforspecifictransactions.Theyoftenusecontracttemplatesornegotiationprocessestoobtaintheconsentofthe businesses. These methods involve signing a document or exchanging emails to indicate acceptance of the terms and conditions.

Third,B2CandB2Be-commercecontractshavedifferentimplications forliability. B2C e-commerce contractstend tolimit the liability of the businesses andfavor theconsumers. They often includeclauses such as disclaimers,limitations ofliability,and arbitrationagreements.Theseclausesaimtoreducetheexposureofthebusinessestolawsuits,damages,orpenalties.B2B e- commerce contracts tend to allocate the liability of the parties according to their respective roles and responsibilities. They oftenincludeclausessuchasrepresentations,warranties,indemnities,andliquidateddamages.Theseclausesaimtoensurethe performance of the parties and compensate for any breaches or losses.

HowtocreateeffectiveandenforceableB2CandB2Be-commercecontracts?

CreatingeffectiveandenforceableB2CandB2Be-commercecontractsrequiresfollowingsomebestpractices.Firstly,youneed toknowyourtargetmarketandlegalobligations,asdifferentlawsmayapplytoonlinetransactionsdependingonwhetheryou selltoconsumersorbusinesses. Additionally,youneedtoconsiderthejurisdictionandchoiceoflawofyourcontractsifyousell across borders or states. Secondly, it is important to use clear and concise language and structure in your contracts so that they are easy to read and understand. You should avoid using jargon, legalese, or ambiguous terms that may cause confusion or disputes. Moreover, it is essential to provide adequate notice and consent by making your contracts visible and accessible before customers enter into online transactions. Furthermore, you should obtain their explicit and informed consent to theterms and conditions of your contracts using clickwrap, browsewrap, or email confirmation. Lastly, you should review andupdate your contracts regularly as they should reflect the current state of your online business and changing needs of customers. You shouldalsomonitorchanges inlawsthat affect onlinetransactionstoensurevalidityandenforceability ofyour contracts.

Esecurity:

Whatisthepointofcybersecurity?

Thequestionmightseembasic,butittouchesononeofthemostimportantissuesfacingcompaniesaroundtheworld.Indeed,thisquestionis socriticalbecause —despiterepeatedattempts toshoreupdigitalsystemsoverthelastfew decades —cybersecurityrisks remain rampant.

In2022alone,atotalof4,100publiclydiscloseddatabreachesoccurred,comprisingsome22billionrecordsthatwereexposed.All thisdespite the fact that organizations around the world spent a record-breaking $150 billionon cybersecurity in 2021.

Softwareitselfischanging,too.Theriseofartificialintelligencein general,andgenerativeAIin particular,isfundamentallyalteringthewaycompaniesusesoftware.TheincreasinguseofAIis,inturn, makingsoftware's attacksurfacesmorecomplicatedandsoftware itself more vulnerable.

How,then,shouldcompaniesgoaboutsecuringtheirsoftwareanddata?

Theanswerisnotthatcybersecurityisapointlessendeavor—farfromit.Instead,whatcompaniesaimtoachievefromtheirsecurityprograms must evolve, just as the way that companies' use of data and software has evolved. It is past time fortheircybersecurity efforts to change, too.

ManagingCyberRisk

Morespecifically,companiescan adapttothegrowinginsecuritiesofthedigitalworldbymakingthreechangestothewaystheygo aboutshoring up their software:

3WaysCompaniesCanImproveTheirCybersecurity

First,cybersecurityprogramsmustnolongerhavetheavoidanceoffailuresastheiroverarchingaim.

Softwaresystems,AI,andthedatatheyallrelyuponaresocomplexandbrittlethatfailureisinfacta featureofthesesystems,not a bug.Because AI systems themselves are inherently probabilistic, for example, AI is guaranteedto be wrong at times — ideally,however,justlessso thanhumans.Thesameholdstrueforsoftwaresystems,notbecausetheyareprobabilistic,butbecauseastheir complexity increases, so too do their vulnerabilities. For this reason, cybersecurity programs must shift theirfocus fromattempting to *prevent* incidents to *detecting and responding* to failures when they do inevitably occur.

Adopting so-called zero trust architectures, which are premised on the assumption that all systems can or will becompromisedby adversaries, is oneof many ways torecognizeandrespondtotheserisks. TheU.S.governmentevenhas a zerotruststrategy,which it'simplementingacrossdepartmentsandagencies.Buttheadoptionofzerotrustarchitecturesisjustoneofmanychangesthatneedto occur onthewaytoacceptingfailuresinsoftwaresystems.Companiesmustalsoinvest moreintheirincidentresponseprograms,redteamtheirsoftwareandAIformultipletypesoffailuresbysimulatingpotentialattacks,bolsterin-house incident response planning for traditional software and AI systems, and more.

Second,companiesmustalsoexpandtheirdefinitionof"failure"forsoftwaresystemsanddatatoencompassmorethanjust security risks.

Digitalfailuresarenolongersimplysecurityrelated,butinsteadnowinvolveahostofother potentialharms,rangingfromperformanceerrors to privacy issues, discrimination, and more. Indeed, with the rapid adoption of AI, the definition of asecurity incidentis itself no longer clear.

Theweights(thetrained"knowledge"storedinamodel)forMeta'sgenerativeAImodelLLaMA,forexample,wereleakedtothepublicin March, giving anyuser theability to run themultibillion–parameter modelon their laptop. Theleak may havestartedas a security incident, but it also gave rise to new intellectual property concerns over who has the right to use theAImodel(IPtheft)andunderminedtheprivacyofthedatathemodelwastrainedon(knowingthemodel'sparameterscanhelptorecreate itstrainingdataandthereforeviolateprivacy).Andnowthat'sit'sfreelyaccessible,themodelcanbeusedmorewidelytocreate and spread disinformation. Put simply, it no longer takes an adversary to compromise the integrity or availabilityofsoftwaresystems;changingdata,complexinterdependencies,andunintendedusesforAIsystemscan giverisetofailuresallontheirown.

Cybersecurity programs cannot therefore be relegated to only focusing on security failures; this will, in practice,makeinformationsecurityteamslesseffectiveovertimeasthescopeofsoftwarefailuresgrows.Instead,cybersecurityprograms mustforma part of broader efforts focused on overall risk management —assessing howfailures can occur and managingthem,regardless of whether the failure was generated by an adversary or not.

This, in turn, means that information security and risk management teams must include personnel with a wide rangeofexpertisebeyondsecurityalone.Privacyexperts,lawyers,dataengineers,andothersallhavekeyrolestoplayinprotectingsoftwareand data from new and evolving threats.

Third,monitoringforfailuresmustbeoneofthehighest-priorityeffortsforallcybersecurityteams.

Thisis, sadly, notcurrentlythe case. Last year, for example, ittook companies an average of 277 days, or roughly9 months,toidentify and contain a breach. And it's all too common for organizations to learn about breaches and vulnerabilities intheirsystemsnotfromtheirown securityprograms,butthroughthirdparties.Thecurrentrelianceon outsidersfordetectionisitselfatacit admission that companies are not doing all they should to understand when and how their software is failing.

What this means in practice is that every software system and every database needs a corresponding monitoring planandmetricsforpotentialfailures.Indeed,thisapproachisalreadygainingtractionintheworldofriskmanagementforAIsystems.TheNational Institute of Standards and Technology (NIST), for example, released its AI Risk Management Framework(AIRMF)earlier this year, which explicitly recommends that organizations map potential harms an AI system can generate anddevelopacorrespondingplantomeasureandmanageeachharm.(Fulldisclosure:IreceivedagrantfromNISTtosupportthedevelopmentoftheAI RMF.) Applying thisbestpractice to softwaresystemsanddatabaseswrit largeisonedirectway topreparefor failuresintherealworld.

Thisdoesnotmean,however,thatthirdpartiescannotplayanimportantroleindetectingincidents.Quitethecontrary:Thirdpartieshavean important part to play in detecting failures. Activities like "bug bounties," in which rewards are offered inexchange fordetecting risks, are a proven way to incentivize risk detection, as are clear ways for consumers or users tocommunicate failureswhen they occur. Overall, however, third parties cannot continue to play the primary role in detectingdigitalfailures.

...

Aretheaboverecommendationsenough?Surelynot.

Forcybersecurityprogramstokeeppacewiththegrowingrangeofriskscreatedbysoftwaresystems,thereismuchmoreworkto be done.More resources, for example, are needed at all stages of the data and software life cycle, from monitoring theintegrity of dataover time to ensuring security is not an afterthought through processes such as DevSecOps, a methodthatintegratessecuritythroughoutthedevelopmentlifecycle,andmore.AstheuseofAIgrows,datascienceprogramswillneedtoinvestmore resources in risk management as well.

Fornow,however,failuresareincreasinglyacorefeatureofalldigitalsystems,ascompanieskeeplearningthehardway.Cybersecurityprograms must acknowledge this reality in practice, if not simply because it is already in fact a reality.

ApplicationareainCybersecurity:

1. Top10ImportantApplicationsofCyberSecurity
2. BenefitsofCyberSecurity
3. DifferentTypesofCyberSecurityThreats
4. WhyDoBusinessesNeedCybersecurity?
5. FinalThoughts
6. FrequentlyAskedQuestions(FAQs)

ViewAll

Agrowingamountofinformationisbecomingdigitalandaccessiblethroughwirelessandwireddigitalcommunicationnetworksinadditiontothepervasiveinternet.Oneoftheprimaryreasonsistherapidlychangingtechnologicallandscapeandthefactthatsoftwareadoptionissteadilyrisingacrossnumerousindustries,includingfinance,government,military,retail,hospitals, education,andenergy,tonameafew.Sincecybercriminalsvalueallextremelysensitiveinformationgreatly,itiscrucialtosafeguarditusingrobust applications of cybersecurity.

Cybersecurityisdefendingsensitivedataandimportantsystemsfromonlinethreats.**Cybersecurity**measures,sometimes referredtoasinformationtechnology(IT)security,areintendedascounterattackstothreats,whethertheycomefrominsideoroutsideofanorganization.Severalorganizationsensuretheiremployeesundergotrainingforthesame.Althoughthe**Cybersecuritycourseduration**mayvary,employeesgetanopportunitytobuildexpertiseinthesubjectandreducecyberattack possibilities.

Top10ImportantApplicationsofCyberSecurity

Cybersecuritythreatschangeovertime,anditisimportantfororganizationstocounterthesethreats.Intrudersadjustby creating new tools and tactics to undermine security when new protections are developed to counter more recent attacks.Yourorganization's cybersecurity is only as strong as its weakest link. To safeguard your data and systems, it's crucial tohaveacollectionofcybersecuritytoolsandtechniquesatyourdisposal.Belowareafewimportantapplicationsofcybersecurity-

1. NetworkSecuritySurveillance

Continuous network monitoring is the practice of looking for indications of harmful or intrusive behavior. It isoften usedinconjunction with other security tools like firewalls, antivirus software, and IDPs. Monitoring for network security may bedonemanually or automatically using the software.

2. IdentificationAndAccessControl(IAM)

Themanagementhascontroloverwhichindividualcanaccesswhichsectionsofthedata.Usually,themanagementregulateswhohasaccesstodata,networks,andcomputersystems.Hereiswhere**cybersecurity**comesintothepicturebyidentifying usersandexecutinganaccesscontrol.Various**cybersecurityapplications**ensureIAMacrossanorganization.IAMmaybe implementedinbothsoftwareandhardware,anditoftenmakesuseofrole-basedaccesscontrol(RBAC)tolimitaccesstocertainsystemcomponents.

Managerscanmanagewhohasaccesstowhat,whentheycanaccessit,andforhowlong,thankstosolutionproviderslikeOkta.

3. SoftwareSecurity

Applicationsthatarecrucialtocompanyoperationsareprotectedbyapplicationsecurity.Itcontainscontrolslikecodesigningandapplicationwhitelistingandmayassistunifyyoursecurityruleswiththingslikefile-sharingrightsandmulti-factorauthentication.WiththeapplicationofAIin**cybersecurity**,softwaresecurityisboundtoincrease.

4. RiskManagement

Riskmanagement,dataintegrity,securityawarenesstraining,andriskanalysisareallcoveredbycybersecurity.The evaluationofrisksandthecontroloftheharmthatmaybedoneasaresultoftheserisksareimportantcomponentsofrisk management.Thesecurityofsensitiveinformationisanotherissuecoveredbydatasecurity.

5. Planningfordisasterrecoveryandbusinesscontinuity

Datarecoveryenablesorganizationstocontinueworkingintheeventofdataloss,assaults,orcalamities.Byregularlydatabackup and spending money on a system that will enable corporate activities to continue, this application offers modelsortechniquesthatmayhelpfirmsmanagewithseveredataloss.Thus,thisapplicationofcybersecurityensuresbusinesscontinuity.

6. PhysicalSecurity

System locks, intrusion detection systems, alarms, surveillance systems, and data-destruction systems are a few examplesofphysicalsecuritymeasures.ThesealloworganizationstosecuretheirITinfrastructure.

7. ComplianceAndInvestigations

Cybersecurityishelpfulduringtheexaminationofsuspicioussituations.Additionally,ithelpstoupkeepandadhereto regulations.

8. SecurityDuringSoftwareDevelopment

The software aids in detecting software flaws when they are being developed and ensuring that regulations and standardsarefollowed. Cybersecurity tools thoroughly test, scan, and analyze the software to identify any bugs, openings, orweaknessesthathackers or competing businesses might exploit.

9. SecurityAgainstDDoS

Cybersecurity aids in providing amitigationsolution to deal with DDoS. Itredirects traffic to other cloud-basedservers andresolvestheissue.

10. ProtectingCriticalSystems

Cybersecurityaidsinpreventingassaultsonhugeserverslinkedtowide-areanetworks.Itupholdsindustry-standard,strictsafety standards for users to abide by cybersecurity precautions to secure the devices. It keeps track of all apps in real time androutinelyevaluates the network security, servers, and users themselves.

BenefitsofCyberSecurity

Thereareseveraladvantagesofusingcybersecurity.Belowareafewofthem-

1. SafeguardsTheReputationOfYourCompany

Databreachesoftendamageyourcompany'simage.Everybusinessinthemarketisvyingfortheclient'sconfidenceaboveallelse.Hence,asignificantdataleakmightreducetheclient'sfaithinyou.Buildingasafesystemandtakingallnecessarystepsare essential for preventing suchdisastrousincidents.

Cybersecurityapplicationsenableyoutohandleauthenticationusingnetworksecurityandcloudsecuritytechnologies. Individualspursuingthe**bestEthicalHackingcourseonline**willdeveloptheskilltoidentifyloopholesinthesystemand safeguardtheircompany'sdata.

2. ShieldsPersonalInformation

Personalinformationisoneofthemostcriticalassetsinthedigitalera.Acybersecurityappmakesitdifficultforavirustoextract or corruptinformation within the system.

3. EnablesWorkersToDoSoSecurely

Everyorganization'sstaffiscontinuouslyatriskofapossiblecyber-attackifthecompanydoesn'thavethebestcybersecurityapps.

4. FacilitatesRemoteWork

ThegigeconomyandremoteworkersnowrequirebusinessestojoinZoomconversationsandsyncalloftheirprocessesanddata.Insuchascenario,cybersecuritytoolsandeffectiveITsupportoptionscansafeguardyourhomeWiFiandblockhackersfrommonitoringortrackingthedataofyouremployees.Itfunctionsasacentralizedsystemthateffectivelysecuresyourdata.

5. ImprovedDataManagement

Businesseswithstreamlined**cybersecurity**maysimplifyandmodifyanyinformation,fromsensitivecustomerdatato individualemployeedata.Theapplicationsimproveprivacy,andoperationaleffectivenessmaybeincreased.Acrossthe**KnowledgeHutcybersecuritycourseduration**,theprofessionalswillbeabletounderstandtheapplicationofcyber securityinreallifeandhowtoutilizecybersecuritysoftwarefordatamanagement.Forthenextstep,checkoutour**guideon howtogetintoCyberSecurity**here.

DifferentTypesofCyberSecurityThreats

Threetypesofattackscounteredby**cybersecurity**are:

- Cybercrimecompriseseloneindividualsororganizationsthatattacksystemsforharmorfinancialadvantage.
- Informationcollectionforpoliticalpurposesisacommoncomponentofcyberattacks.
- Cyberterrorismaimstocompromiseelectronicsystemstoelicitfearorpanic.

Belowaresomeofthemostcommoncybersecuritythreats-

1. Viruses
2. DDoS
3. Malware
4. Worms
5. Trojan
6. Phishing
7. **Socialengineering**
8. Ransomware
9. **SQLInjectionWhyDoBusiness**
esNeedCybersecurity?

Therecenthigh-profilesecuritybreachesofcompanieslikeEquifax,Yahoo,andtheU.S.TheSecuritiesandExchangeCommission (SEC),which lost extremely sensitive user data and suffered irreparable damage to its financesandreputation,indicatesthealarmingneedforsoundcybersecuritystrategies.Hence,itisintegraltoensureyourcompanyhasthenecessary**cybersecurity tools**and techniques in place.

AnIBM estimatefrom2021showsthat cybercrimescostfirms$4.24milliononaverage.By 2025, itispredictedthatcybercrimewill cost $10.5 trillion annually.

Manybusinessesoverlookthe**needforcybersecurity**andbecometargetsofattacks.Becausetheydon'tconsiderthem requiredexpenditures,sotheydon'tevenadoptthemostfundamentalsecuritymeasures.

Incontrast, many firmsthroughoutthe globe thatare awareof theircyberdefensehaveemployedtechnology toleveragequicklyexpanding technological standards to become more resistant than ever.

Lookingtoboostyourcareer?Get**ITILcertificationtraining**andunlockendlessopportunities.UpgradeyourskillsandbecomeanITIL expert. Join now!

FinalThoughts

Thefightagainstcybersecurity is never-ending.Soon,therewon'tbea conclusiveanswertotheissue.Thecomplexity ofITsystems,theintrinsicnatureofinformationtechnology(IT),andhumanfallibilityinformingjudgmentsaboutwhatactivitiesandinformationaresafeorhazardousfromacybersecurityviewpointaretheprimarycausesof**cybersecuritychallenges**.

There are no magic solutions or even combinations of solutions (cybersecurity applications) that will "fix the issue"permanentlysince none of these variables is anticipated to alter shortly.

InnovationcreatesnewITapplications.However,italsocreatesnewopportunitiesforcriminals,terrorists,andotheradversaries to operate. As a result, improving a system's cybersecurity posture must be seen as a continuous effort rather thansomething that canbe completed once and then ignored.

FrequentlyAskedQuestions(FAQs)

1. WhatarethefivebenefitsofusingCybersecurityApplications?

Thereareseveraladvantagestousingcybersecurityapplications.Belowareafewofthem:

- Safeguardsthereputationofyourcompany
- ShieldsPersonalInformation
- Enablesworkerstodososecurely
- FacilitatesRemoteWork
- ImprovedDataManagement

2. Whatareexamplesofcybersecurity?

Network securityexamplesincludefirewallsthatpreventillegalaccesstoanetworka ndantivirus.AntispywaresoftwareandVPNs(VirtualPrivate Networks)areother examplesusedforsecure remote access.

3. Whatisanapplicationsecurityexample?

Hardware,software,andprocessesthatdetectorreducesecurityvulnerabilitiesfallunderapplicationsecurity.For example,hardwareapplicationsecurity safeatur eofroutersthatblocksInternetusersfromreadingacomputer'sIPaddress.

4. Howdoescybersecuritywork?

Allof thecomputers,networks,andsoftwarethatacorporation usesareprotectedbyvariouslevelsof cybersecurity.Thecompany,itspeople,itsprocesses,anditstechnologymustallbeintendedtooperateinunisontoprovideaunited defenseagainstprospectivecyberattacks.

When cybersecurity systemsare working effectively, they can identify,look into,and fix anysystemicflawsor vulnerabilitiesbefore ahacker or malicious software can take advantage of them.

5. Whichappisbestforcybersecurity?

The market has several applications for cyber security. Avast is one of the best cybersecurity apps for securing yourdevicefromvirusesandotherdangers.AneffectivefreeantiviruscalledAvastwillalertyouwhenmalwareandadwarehavebeeninstalledan dare invading your privacy.

Law Key Issues on Cyberspace Taxation Dr. PRADEEP K.P. 24 February 201121 min readShareBookmark Paper presented inInternationalCyberlawSeminaronCyberspaceUsagesandDisputes,Kochi,Kerala,IndiaCyberspaceisavirtualtradingshop, from where income is generated, sale and purchase are transacted, service to clients and entertainment and luxuries to the customersareoffered.Consideringtheenormousscopeforcommercialactivities,itcanbeameadowoftaxationgivingawider scope to the State to generate public revenue.

1. Introduction Tax is a mandatory imposition by the sovereign without any guaranteeofspecial benefits. The imposition of tax is a constitutional function. Such an imposition maybe either upon person or property or privileges or occupationsorenjoyments of the people. Obviously,the primary implication andobject of taxation is to raise money for the purpose of the Government, bymeansof contributionfrom individual persons. Whilelevying a tax, the State, to someextent, brings in measures to regulate the business activity ortheconsumptionofacommodityorserviceorevenaccumulationofwealthinthehandsofafew. Neutrality is an essential precept of taxation which proposes that economically similar income should betaxedsimilarly. Thusthetaxationprinciplesthatapply totheconventionaltaxationeventsshouldalsoapply to,inthesamespiritandforce,inthecross-bordertransactionsconnectedtocyberspace.Isnotacyberspace,adaptable to the taxingpowerof the sovereign? Thisisa debatable question in the current scenario. The e-spacehasavitalroleinthecontemporarysocietyandmainlye-commercepresentsenormouschallengesto the internationaltaxregime, whichfocusesonterritorialand personalbasesoftax jurisdiction. 2. Scope for TaxationinCyberspaceE-commerceisoneofthelatest contributionsoftechnologicalgrowth. E-commerce consistsofthebuying,selling,marketingandservicingofproductsorservicesoverthecomputernetworks. Originally,internetfacilitatedcommercialtransactions,includingsale,electronically.Itwas,usually,for limited purpose, by using technology like Electronic Data Interchange, to send the commercial documents

like purchase orders or invoices electronically, in the course of sale of goods. But, it has developed from a mere means of communication to a mode of carrying the real commercial activity itself. Of course, Income generated by an e-service provider or an e-commerceman is taxable under thedirect taxation, Income Tax Act.The creation ordevelopmentof software can be a point of taxation underthe excise law. Software canbedevelopedandinstalledbysharingthecomputerorserver,evenbyaremoteaccess,throughateamviewersolution.Transferofrights,eitherunderleaseorunderasale, inthecourseofe-commercebusinesscanbe taxedunderuseorconsumptiontaxorsalesandvalueaddedtax.Aserviceproviderisliabletopaytaxunder theservicetaxregimeforhisturnoverderivedfromtheservice,whichhehasdoneinthecyberspace.The ongoingdevelopmentininformationtechnologyfacilitatessaleandpurchaseofgoodsandservicesovertheWorld WideWebviasecureservers,speciallydesignedforconfidentialorderingdatakeepingcustomerprotection,andwith thehelpofe-shoppingcardsandwithelectronicpayservices,likecreditanddebitcards. Anyproductthatcanbedigitalisedisamenabletosaleanddelivery,electronically.Thiswouldincludebooks, newspapers,CDs,motionpictures,photographs,airlineandmovietickets,andvideoandsoundrecordings. Even thesaleable commodities like patent, designs and trademarks, which aredigitally convertible can also betheobjectofelectroniccommerce,whetherintheformofatotaltransferorintheformofpartialtransferofrights. E-commerce has a vital role in the areas of entertainment industry. A wonderful movie having international recognitioncanbedownloadedandseenthroughwebsitesbypayingcharges.Anybooksattained worldwide popularitycan be read in a website by viewersby paying charges, all over the world. A newlyintroduced song of an admired pope singer can be accessed and stored by his admirers around the world, through the browsing and downloading. While watching such a movie or reading such a book or listening suchasong,certainlytransferofinformationtakesplace,eitherassale,orasservice.3.Issuesin CyberspaceTaxation.Likeanyotherlegalsystems,therearechallenges,inevitableinthefieldofcyberspacetaxation also. Suchtax challenges areuniquethrough out theworld, evidently in gainingjurisdictiontoset therules, tojudgeandenforcethemunicipaltaxationlawstothecyberspace.Thereareotherareaswhich raisecrossboarderlegalissueslike,conflictsinapplyingdifferentprinciplesoflaw.Ininternationaltaxation,income earned from the economic activity by a resident of one country in the territory of another country can be subject to levy oftax onincome in both the countries. Thehomestatejustifies inlevyingtax onthe basis of residencerule,however thehoststatemayimposethetaxonthebasisofsourcerule.3(i).Jurisdictional Issues in E-commerce When e-commerce enables transaction of sale and services, across borders there is unavoidableambiguityregardingjurisdictionandtheapplicabletaxlaw.Partiestoacybergenerated contract may be located in different jurisdictions which may have serious implications in the interpretation and enforcement of the law.Is it the municipal law of the country or the law of other party having foreign jurisdictionthatcoversthefield?Thetraditionalrulesofprivateinternationallawstate thatthejurisdictionofacountry extendsonlytoindividualswhoarewithinthecountryortothetransactionsand events that occur within the natural boundary of the country[1].

2. Therearesomeimportantprinciplesgoverningtheissues.3(i)(a).TheoryofMinimumContactsThetheoryofminimumcontactswouldmeanthatevenifapersonisnotphysicallypresentinacountry,hecanbe proceededinthatforeigncourtaslongashiswebsitehasminimumcontactswiththatcountry.Thisgeneral lawhasuniversalapplication.Normallyaserviceprovidermayinsertappropriatechoiceoflawintheonlinecontracts, including specification of the jurisdiction to which the parties to the contract would be subject to andsuch clauses are bindingupon the parties[2]. 3(i)(b). SourceandResidence Principles. The principles of source or residencegovernthejurisdictionoftaxingsubject,apparently,indirecttaxation.Asperthis principle,theincomeissubjecttotaxwheretheincomeissourcedorthesubjecthastheresidence.Howeverintaxing of E-commerce, application of the principles may hit the regional balances, at least in cases where majorportion of goods are sourced in one region and largely consumed in another region. In cases of countries, which are havingvital monopoly on software and other digital exports, the application of source principles in E-commerce sale will definitely result in regional imbalance, if the sales are not attributable through apermanentestablishmentintheothercountry.Theprincipleofresidenceisalsoinapplicableincertain areas of taxation that taxes on E-commerce sales, since majority of e-commerce service providers exist in cyberspaceonly.Ofcourse,insuchcasestheresidenceofsuchsellerscanbeattributabletothe locationoftheserverthathoststhehomewebsiteoftheseller.3(i)(c).ConceptofPermanentEstablishment. The concept of ‘Permanent Establishment’ suggests that if the activity passes the permanent establishment in thesourcecountry,thatcountrywouldhavetheprimaryrighttotaxtheactivity.Thepermanent establishment is defined in the OECD Model Tax Convention to mean, the fixed place of business through whichthebusinessofanenterpriseiswhollyorpartlycarriedon.Itmaybeaplaceofmanagement,abranch,anoffice, afactory oraworkshop.Wherea personisactingonbehalf ofan enterpriseand hashabituallyexercisedan authority to conclude the contracts in the name of such enterprise, it is deemed that such enterprises shall haveapermanentestablishmentinsuchplace.Howeverifabroker,generalcommission agentoranyotheragentofanindependentstatusisactingintheordinarycourseoftheirbusiness,itcannotbesaid that the enterprise is having apermanent establishment in such place, merely for thereason thatbusinessiscarriedthroughsuchpersons.Whenaforeignerleavesthemanagementofhisdomesticshare portfoliowithastockbrokerinacountry,suchagencywillnotconstituteapermanentestablishment.Thusawebsite hosted on a server owned by a domestic independent agent like an ISP (Internet Service Provider), would notconstituteapermanentestablishment.Avendor’s homepageon the internetand theaccessofthe internet provided to that homepage do not give rise to a permanent establishment, since the vendor does nothavecontroloveranyoftheappliancesnecessaryfordatatransmission,inacountry.Adifferent version is that a web page is likely to constitute a permanent establishment in the country where the host computerresides.Itisbecauseawebpagecanhaveaphysicalpresence,asitismadefrombinaryordigital codeandishousedonamagneticsurface,usuallyadiskofsomekind.Suchabinarycodeisviewableusing the computerandcommunicationdevice.3(i)(d).TheoryofPhysicalPresence.Theprimarydeterminative andwidelyacceptedfactorregardingexigibilityoftaxoncyberspaceore-commerceisthephysicalpresence of seller or service provider in the customer's state. For determining whether seller or service provider has physical presence, or a level of activity, the significant tests are that either the entity must be owning or rentingpropertyinthatstateorhavingawarehouseorafulfilmenthousethatmaintainsinventoryforseller in that state or having employees in that state or promoting his business in that state through something likeatradeshow.TheCourtsintheUnitedStatesmaintainasensiblelegaloutlookinthisregard.According to them when the seller or service provider has no activity in the location, but merely a web presence, it would not bring them with in the state's jurisdiction to proceed against the seller. In National Bellas Hess, Inc'scase[3], theU.S SupremeCourthasheld thatthesellerscould berequired topay user taxesonlyinthe states where they havemaintaineda certain level of physical presence. This was a majorhit on the state's powertotax on the inter-state mail orderorcatalogue sales. Later the U.S. Supreme Court in Quill'scase[4] has held that it is for the Congress to decide the scope of nexus theory to protect the interest of State's revenue, though. 3(ii). Issues in Identification of Parties Identity of parties to a contract is one of the keen issuestoberesolvedwhileperforminge-contracts.Unlikecommunicationsofofferandacceptancethrough postal means, in internet communications, it is not possible to locate the exact place of the parties, in the first instance. It can be possible only through decoding of protocol addresses and through other technological solutions, which are time consuming and highly technical. Transactions on the internet, particularlyconsumer-relatedtransactions,resultinginsaleorservicecontracts,oftenoccurbetweenparties who have no pre-existing relationship, whichmay raise concernsof theperson's identity with respect to issuesof the person's capacity, authority and legitimacy to enter into a contract.

3. 3(iii).RelativeIssuesofE-CommerceTaxationThephysicalsupervisionsoverthemovementofgoodsor servicearesomeoftheprimeconcernsintaxinge-commerce.Ine-commerce,themajorityofsalesorservice are relatingtointangiblegoodsthatarewithouttheneedtoprovidetangiblepersonalpropertytothe customer; sale and service can be effectedthrough transferof intangible properties. 3(iii)(a). Administration ofTaxInthetraditionalsystemoftrading,withrespecttothemainstreet-retailers,theadministrationoftaxiseasier. Thetaxonsaleorserviceis,ofcourse,anindirecttaxanditistheprimarydutyofthetradersor serviceproviderstocollectandremitthetaxtotheStateex-chequer.However,thee-commercebusinessmanmaynotbeobligedtocomplywithsuchstatutoryrequirementsintheabsenceofregularsupervisionofhis business.Theroleofconsumptiontax,inrelationtotangibleproperties,issignificantinsuchsituations.Theliability, insuchcasescanbefastenedontheimporterorthepersonwhoconsumesthegoods.Incasesof electronicsupplyofintangiblegoods,domestically,thereisnotmuchdifference,asthedomesticdealerhas anobligationtocollectthetaxandsuchtradesaresubjecttotaxauditalso.Butdifficultymayarisewhenthe trader destroys his back-up. In cases of electronic supply of intangible goods by a foreign supplier, such supplies satisfytherequirementofimportsaleandthetaxcanbeleviedontheimporter,whoconsumessuch goods.Suchusetaxisusual,whenthesellerisincapableoftaxingthesale,becausehehasnonexus withthedestinationstate.ItisanundisputedfactthatE-commerceishavingadramaticimpactonalmostall aspectsofbusiness.Ithasopenedaglobalmarketwithglobalsuppliersacrossthenations.Thoughregulatorymeasures were introduced to regulate and protect the issues of intellectual property rights in the field of cyberspace,thelawontaxadministrationisnotyetfullydeveloped.Theconsequenceisthatthe technologically advancedandhigh earningsociety, who builds e-commerceas parallel market, is out oftax administration.Soeithertheconceptofsaletaxshouldfurtherbemodifiedtocoverthefieldorthetaxation jurisprudenceshouldadvancefurtherbydevelopingalternativedevicestofillthegap.Whenane-commerceservice providerprojects certain information to its customers, through thewebsite, bychargingmoney through credit cardpayments, andthecustomer only exploringsuch information totheir mind oreven writingdown itintotheirnotebooks, canitbe said thatanytransfer ofgoods are effectedbetweentheweb siteownersandcustomer.Furthermore,ameredownloadmaycreateavirtualrecyclebinwithunnecessarydownloads in temporary internet folders or cookies, a temporary storage, which the person really did not intend. In fact, whetherthe taxman can tax such downloads, naming it as sale orservice or under the guise ofdeemedincomearisingfromit.Itisasifasoftwareishostedinaclient'scomputerfromaremote programmingterminallocatedinfarawayplacetoconstitutetransferofintangiblegoodsthrough communicationdevices.Itisthelawthatevenifitisnotrecordedintangiblemedia,butonlypassedthrough a deputing personal, there is transfer of property in goods exigible to the sales tax. A momentary service of passing of information, which is a valuable intangible property, can thus be treatedas sale for the purpose oftaxation.Thetaxingauthoritiesareseriouslythinkingtocurbthesituationoftaxavoidanceinlike transactions.Whiletaxingacommodity,asanarticleofmerchandise,theremustbeanincidencefortax,i.e.,thesale.It isnotthatthecommodityissubjectedtotax,butittransferassalewhichissubjectedtotax.In imposingthesalestax,oneofthedifficulties,whichconfronttheTaxman,liesintheselectionofthepointof timeatwhichthetaxshallbeattachedandbecomedue.Inthecaseofanordinaryretailsaleforcashacross thecounterofshop,thestagesofagreement,appropriationofthegoodstothecontract,delivery,payment ofthepriceandpassingofthepropertyareallpracticallysimultaneous[5].Ontheotherhand,intransactionslikeE-commerce,whicharemorecomplicatedinnature,itisdifficulttofindoutthesestages independently.3(iii)(b).SitusofBusinessWhentheactofsaleorserviceisthesubjectoftaxation,theplace ofsucheventhasrelevance.Theremustbeasitusofsaleorservice.Saleconsistsofanumberofingredients, suchasexistenceofgoodswhichformthesubjectmatterofthesale,abargainorcontractofmutualconsent, which, when executedwill resultpassingofthe propertyin thegoodsfora price,thepaymentora promisetopay the price and the passing of title[6].

4. When all of it takes place simultaneously, there is no difficulty to ascertain the place of sale. When one or more ingredients take place at different places, it is difficult to find out the situs of sale.In e-shopping, the situs of sale is not certain. Goods can be ordered from one place, payment can be effected from another placeandthegoodscanbeaccessedfromaplaceotherthantheabovetwo.Therearecumulativeincidents taking place to finalize the sale of the goods. Can there be levy of sales tax in all places?When the sale occurswithrespecttoaphysicalsubstance,andthesalebeingproximatecauseofmovementofgoodsfrom oneplacetoanother,itiseasytofindoutthephysicaltransferofgoodsbywayofdelivery.Itisnotpossible to adoptthis principle, when intangible properties are transacted through the cyberspace.3(iii)(c). Culmination of Contract A binding contract is constituted by acceptance of an offer.The acceptance must bereachingtheselleratthetimethecontractiscompleted.Duringelectronicofferandacceptanceanumber of questions will arise. Can a mere action of downloading be considered as the acceptance? The user may discardasurfedmaterial,visuals,orwritings.Aclickontheoptionsinthewebsitecannotbeafullacceptance of the information, though a seller anticipates the placing an offer through the website. Without the use of encryption technology, the reliability and acceptability of email, is an added difficulty. In systems in which electronic messages are sent, over communication networks, it is certainly possible forsomeone to prepare and transmit an E-mail message or an acceptance and to make it appear that it came from someone other than the true maker.When authenticity of generation of messages, itself, is doubtful, it is not easy to deal with the taxing subject for taxation, on the basis of such mail orders.

electronicpayments:Haveyoueverwonderedwhat'sinvolvedincreditcardprocessing?Everycreditcardtransactioninvolvesfourparties:The customermakingthepurchase,themerchantreceivingpaymentforthepurchase,thebankthemerchantprocessorusesforcredit cardprocessingservices(acquiringbank),thebankthatissuedthecustomer'screditcard(issuingbank).

HowDoesCreditCardProcessingWork?

Acquiringbanks(alsocalledmerchantbanks)contractwithmerchantstooperateaccountsthatallowthemerchantstoaccept creditcardpayments.Acquiringbanksdepositfundsforcreditcardpurchasesintomerchants'accounts.Theyalsofurnish merchantswithcreditcardprocessingsoftwareandequipmentsuchasamerchantprocessor,creditcardreaderandterminal,as wellasprovidingcustomerservice,promotionalmaterialsandothercreditcardprocessingservices.

Anymerchantwhowishestoacceptcreditcardpaymentsmusthaveamerchantprocessoraccount.Amerchantaccountisan unsecuredlineof credit that pays amerchant forcustomerpurchases.Thepayment is actuallyaloantothemerchant'saccount fromthatmerchant'sacquiringbank.Inotherwords,theacquiringbankloansmoneytothemerchanttocoverthecostof customers'credit card transactions.

Afteracreditcardtransactioniscomplete,themerchantwillhavelessmoneythantheoriginaltransactionamountbecauseboth theissuingbankandtheacquiringbankwillchargethemerchantfeesfortheirservices.Thesefeesincludeapercentageof each transaction,andthehigherthetransactionamount,thehigherthefee.Themerchantmayalsobechargedfixedfeesforeach transactionbytheissuingbank andtheacquiringbank.

WhatYouNeedtoKnowAboutCreditCardProcessing:

Ifyouwanttosetupamerchantaccountforcreditcardprocessing,youprobablywonderaboutthecreditcardfeesyouwillbe charged.Themostimportantdeterminantofhowhighyourfeeswillbeisthetypeofbusinessyouarein.Certainbusinesses are morelikelythanotherstosufferpaymentdisputesandchargebacks,sotheirtransactionsareconsideredriskierbyissuingand acquiringbanks.Businesseswiththeseriskiertransactionsarethereforechargedhigherfeestooffsettheriskofchargebacks.

Chargebacksarewhathappenswhenacustomersuccessfullydisputesacreditcardfeestransactionwithyourbusiness.Thesafesttransactions,as farastheissuingandacquiringbanks areconcerned, takeplacewhenthecardholderswipes his orherown cardinthecreditcardreaderandsignsthereceipttopayforgoodsthatareinexpensiveandnotlikelytogeneratecomplaints. Restaurants,gasstationsandcarrentalagenciesallfallintothiscategory,andbecausetheirchargebackriskislow,theypaylessinfeesfor creditcardprocessingtransactions.

Theriskofachargebackishighestwhentransactionsarecompletedviathe Internetorbyphone.Theriskisevenhigherifthe transactionsareexpensive,involveshippingandthebusinessisonethatissubjecttocomplaints.Thebottomlineisthatwhena merchant appliesforcreditcardprocessingservices,thebusinessthemerchantisengagedinfiguressignificantlyinthefeesthat themerchant will becharged.

WhoNeedsCreditCardProcessingCompanies?

Anymerchant,whetherdoingbusinessinaphysicallocationlikearetailstore,avirtuallocationlikeanonlinewebsite,orbyphone ormailorderneedscreditcardprocessingservicesiftheywishtoserveallpotentialcustomersandremaincompetitive.

Althoughyou,asamerchant,willpayacertainpriceforcreditcardprocessingservices,thebottomlineisthatyoucan'treallybe successfulinyourbusinesswithoutit.However,duetothevariabilityinpricingforcreditcardprocessingservices,youcanshop aroundforthebestdeal.Justbesurethatanyquotesyoureceiveincludealltheratesandfeesyouwillbecharged.

Leadersisoneofthebestcreditcardprocessingservicesintheindustry.It'sbeenaroundfor20years,anditsparent companyisthereputablePaysafeGroupSubsidiary.Leadersgivesbusinessesalotofreasonstoloveit,including someofthebestcreditcardprocessingratesintheindustry.We'retalkingaboutratesthatstartatjust0.15%.Plus, Leadershasa98%approvalrating.So,businesseshavingahardtimegettingthegreenflagwillfindLeaders'process refreshing. What'smore,Leadersoffersasolid$500Assuranceguarantee.Thisstatesthatifthecompanycan'tsaveyoumoney withinthefirst6monthsofyourcontract,you'llbeawarded$500incompensation.Leadersworkswiththereliable Cloverpointofsalesystem,anditalsointegrateswithQuickBooks.NewSMBswillappreciatethehelpfulglossaryof termsand24/7/365customerservicefortroubleshootinganyissues.Additionally,Leadersoffersvalue-addedservices suchasbusinesscashadvances,loyaltyprograms,giftcards,checkguaranteeservices,andpointofsalesystems. Paysafeisacomprehensivepaymentsolutionthatistransforminghowbusinesseshandletransactions.Itacceptsglobal paymentsin17currencies,includingcreditcards,debitcards,digitalwallets,POSsystems,cashcards,andinstallment payments.Thescale-basedpricingstartsat15%forlowvolume,3.9%pervolume,and9.5%forhighervolume.There's alsoafixedfeeof1.5eurospertransaction.Paysafeoffersvariousservices,includingonline,digitalwallet,andinpersonpayments,andadditionalbenefitslikePOSsystems,receiptmanagement,andcurrencyconversion.Thismakesit aversatilechoiceforbusinessesof allsizes andtypes.

Paysafeoffersseveraltoolstoassistbusinesseswiththeirin-storepaymentprocessing.Oneofthenotableequipment offeringsisPaysafe'sAndroidtabletPOS(PointofSale)system,whichfacilitateson-the-spotpaymentacceptance.This POSsystem,combinedwithPaysafe'ssophisticatedin-storepaymentstructure,allowsbusinessestoprovidetheir customerswithvariouspaymentoptions,includinginstallmentpaymentsandmobilepurchasing.Fordetailedpricing, contact Paysafe directly for a tailored quote.

MerchantOneisacreditcardpaymentprocessingcompanythatofferssolutionstosmallandlargebusinessesin variousindustries.Thecompanypartners withClovertoresellitsstate-of-the-artPOSsystems,providesitscustomers withfreetrainingonusingthem,andservicesthehardwarein-house.Thisensuresahigh-qualityuserexperience. WhileMerchantOnehasexcellentreviewsonTrustpilot,severalcomplaintsindicateissueswithcustomerservice, billing,andcontractterms.Nevertheless,MerchantOne’sdedicatedmanagerswillrespondtoqueriesandguideyouonsettingup your account and processing transactions.

WhywechoseMerchantOne-WechoseMerchantOnebecauseit’sabletoprocessbothPOSandmobilephonecredit card payments.

Ourexperience-WelikedthatMerchantOneprovidesadedicatedaccountmanagerandofferslowercardpayment processingfeesthansomeofitsrivals.

SupplyChain:

Overview

- NISTCybersecuritySCRMFactSheet(05/12/22)
- NIST updates Cybersecurity Supply Chain Risk Management Practices for Systemsand Organizationsguidance in NIST SP 800-161r1, which also helps fulfill NIST's responsibilities under E.O. 14028. (05/05/22)
- Seethecommentsreceivedfrom132organizationsandindividualsinresponsetoarecentRFI(2/22/22)onEvaluatingand ImprovingNISTCybersecurityResources:TheCybersecurityFrameworkandCybersecuritySupplyChainRiskManagement

Information,communications,andoperationaltechnology(ICT/OT)usersrelyonacomplex,globallydistributed,and interconnectedsupplychainecosystemtoprovidehighlyrefined,cost-effective,andreusablesolutions.Thisecosystemis composed of various entities with multipletiers of outsourcing, diverse distribution routes, assorted technologies, laws, policies, procedures,andpractices,allofwhichinteracttodesign,manufacture,distribute,deploy,use,maintain,disposeof,andotherwise manageproductsandservices.TheseaspectsofthesupplychainincludeIT,OT,Communications,InternetofThings(IoT),andIndustrial IoT.

TheNISTCybersecuritySupplyChainRisk Management(C-SCRM)programhelpsorganizationstomanagetheincreasingrisk of supply chain compromise related to cybersecurity, whether intentional or unintentional. The factors that allow for low-cost, interoperability, rapid innovation, a variety of product features, and other benefits alsoincrease the risk of acompromiseto the supply chain, which may result in risks to the end user. Managing cybersecurity risks in supply chains requires ensuring the integrity, security, quality and resilience of the supply chain and its products and services. Risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cybersecurity-related elements of the supply chain.

C-SCRM involves identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT/OTproductandservicesupplychains.Itcoverstheentirelifecycleofasystem(includingdesign,development,distribution,deployment,acquisition,maintenance,anddestruction).NISTconductsresearch,providesresources,andconvenes stakeholders to assist organizations in managing these risks.

TwonewNISTeffortsrelatetotheMay12,2021ExecutiveOrder14028,ImprovingtheNation’sCybersecurity,and aNationalInitiative for Improving Cybersecurity in Supply Chains.

NISTApproach

NIST is responsible for developing reliable and practical standards, guidelines, tests, and metrics to help protect non-national security federal information and communications infrastructure. Private sector and other government organizations also rely heavily on these NIST-produced resources. That includes organizations developing or using information, communications, and operational technologies which depend upon complex, globally distributed and interconnected supplychains.

Since 2008, NIST has conducted research and collaborated with a large number and variety of stakeholders to produce informationresources whichhelporganizations withtheirC-SCRM.Bystatute,federalagenciesmustuseNIST's C-SCRMand other cybersecurity standards and guidelines to protect non-national security federal information and communications infrastructure.TheSECURETechnologyActandFASCRulegaveNISTspecificauthoritytodevelopC-SCRMguidelines.NIST also is a member of the Federal Acquisition Security Council (FASC).

NIST has given several grants to conduct research in this area as well as to develop a web-based risk assessment and collaborationtool.

Managing cybersecurityrisk in supply chains requires ensuring the integrity, security, quality, and resilience of thesupply chain and its products and services. NIST focuses on:

- **Foundational practices:** C-SCRM lies at the intersection of information security and supply chain management. Existing supply chain and cybersecurity practices provide a foundation for building an effective risk management program.

- **Enterprise-wide practices:**Effective C-SCRM is an enterprise-wide activity that involves each tier (Organization, Mission/Business Processes, and Information Systems) and is implemented throughout the system development life cycle.

- **Risk management processes:** C-SCRM should beimplemented as part of overall risk management activities. That involves identifying and assessing applicable risks and determining appropriate response actions, developing a C-SCRMStrategyandImplementationPlantodocumentselectedresponseactions,andmonitoringperformanceagainst that plan.
    - **Risk:**Cybersecurity-relatedsupplychainriskisassociatedwithalackofvisibilityinto,understandingof,and controlovermanyoftheprocessesanddecisionsinvolvedinthedevelopmentanddeliveryofcyberproducts and services.
    - **ThreatsandVulnerabilities:**Effectivelymanagingcybersecurityrisksinsupplychainsrequiresa comprehensiveviewofthreatsandvulnerabilities.Threatscanbeeither“adversarial”(e.g.,tampering, counterfeits)or“non-adversarial”(e.g.,poorquality,naturaldisasters).Vulnerabilitiesmaybe“internal”(e.g., organizationalprocedures)or“external”(e.g.,partofanorganization'ssupplychain).

- **Criticalsystems:**Cost-effectivesupplychainriskmitigationrequiresorganizationstoidentifythose systems/components that are most vulnerable and will cause the largest organizational impact if compromised.

ElectronicDataInterchange(EDI):

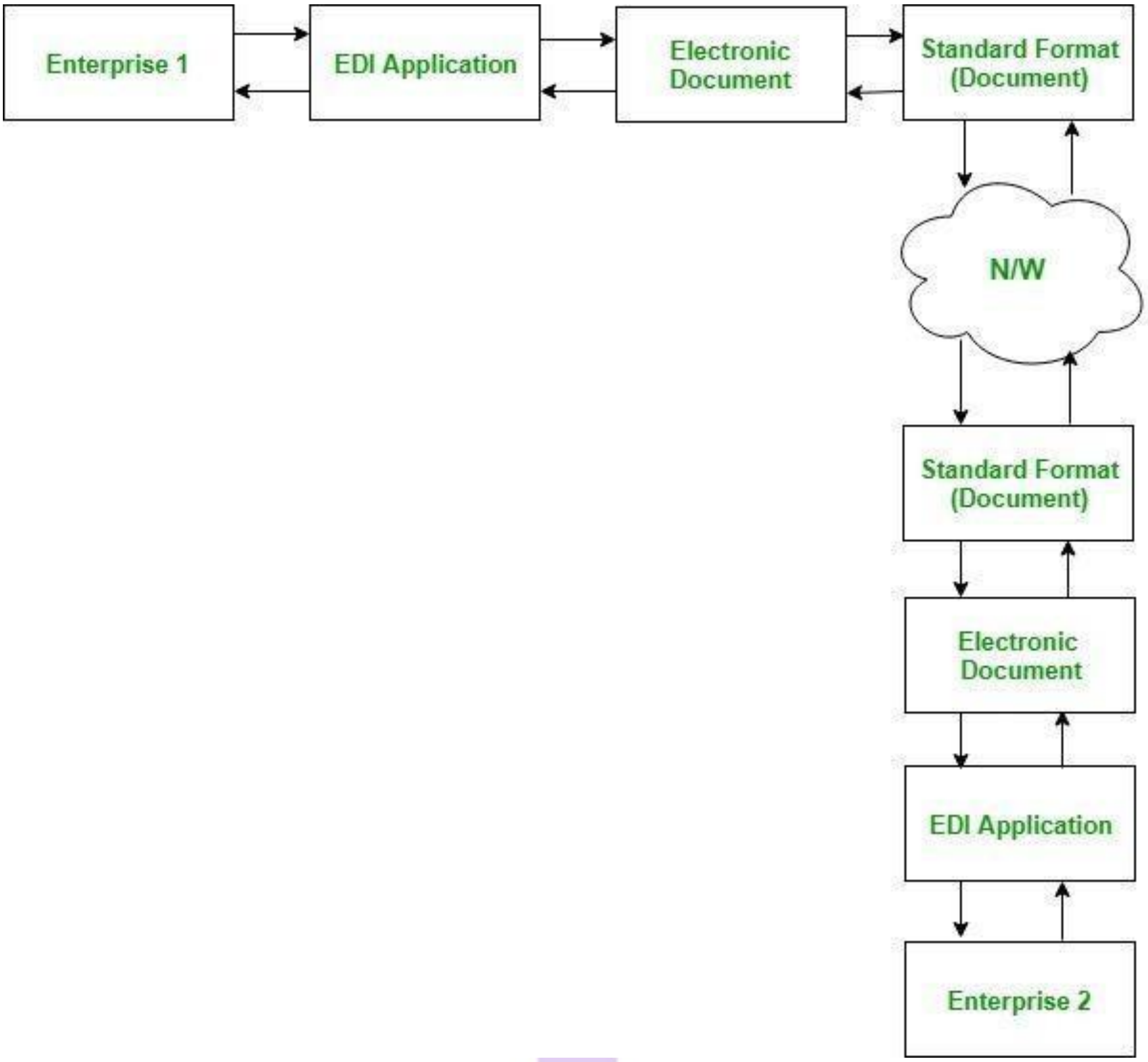
- Read
- Discuss
- Courses

Electronic Data Interchangeis a technique for computer to computer exchange of business documents in a standardelectronicformat between business partnersor companies. Companies useEDI systems for exchanging business informationautomatically bycomputer systems as transactions without paper and hence minimizes or completely eliminates the humanintervention. Electronicdata interchange is generally used for B2B transactions.

CommonEDIdocuments:

1. Shippingrequests
2. Invoice
3. Acknowledgement
4. Purchaseorder

EDIsystem:



BoththeenterpriseshaveEDIapplicationsinstalledintheirsystems.Enterprise1usesitsEDIapplicationtogenerateanEDIdocumentthatitwanttosharewiththeotherenterprise.TheformatofthisEDIdocumentmustbethestandardformatthathasbeendecidedbythetwoenterprisesforsharingEDIdocumentsduringtheirdeals.Thisdocumentissharedwiththeotherenterpriseoverthe network. The document is received by the Enterprise 2 in the standard formaton the EDI application. This is how the twoenterprises exchanges business documents electronically and minimizes or eliminatesthe human interventions.

Advantages:

- Asitisdirectcomputertocomputertransactionsystem,itishighspeed.
- Duetoreducedhumanintervention,itisveryaccurate.
- Simpletouse.
- Highlysecure.
- Reductioninpaperwork.
- Costeffective.

WhatisEDI(ElectronicDataInterchange)?

- Read
- Discuss
- Courses

Introduction:

Electronic Data Interchange (EDI) is a computer-to-computer exchange of business documents in a standard electronicformatbetween two or more trading partners. It enables companies to exchange information electronically in a structuredformat,eliminating the need for manual data entry and reducing the cost and time associated with paper-based transactions.

EDI was first introduced in the 1960s as a way for companies to exchange business documents electronically. Over time,thestandardization of EDI formats and protocols has enabled businesses to integrate their internal systems with those of theirtradingpartners, improving efficiency and reducing errors.

EDItransactionscanincludepurchaseorders,invoices,shippingnotices,andotherbusinessdocuments.TheEDIstandarddefinestheformatand content of these documents, ensuring that they are easily interpreted by both the sender and the receiver.

EDIhasbecomeanimportantpartofmanybusinesses,particularlythoseinthesupplychainandlogisticsindustries.Itallowsforfaster and more accurate processing of transactions, leading to improved customer satisfaction and increased profits.

ItistheworldoftheInternet,knowinglyorunknowingly,everyoneisattachedtotheinternetandisdependentontheinternet.Today,almostallthe workisdonethroughtheInternet.DigitalIndiaisoneexampleofhoweverythingisgoingtobedonethroughtheinternetinthe upcomingyears, notonlyintheupcomingyears,evenrightnow,mostoftheexchangeofcommunicationisdonewiththehelpoftheinternet, whether itischattingonWhatsappwithfriendsor sendingimportantinformationthroughthemail, alltheworkand communication is mostly done through the net.

WhatisE-Commerce?

E-Commercestands forElectroniccommerce,whichmeansbuyingorsellinggoodsthroughtheInternet.ThebiggestadvantageofE-CommerceinthiseraisTimeSavings,notonlythatasacustomer,onemajoradvantageisthatthecustomerreceivesalotofdiscountson theproducts they want to buy.

Intermsofbusiness,abusinessmannotonlycanexpandthemarketallover thecountrybutalsoallaroundtheworld.Businessesalso do not need to put too much effort into Branding.

OnemajorthingthatcomestoplayitsroleinE-

Commerceiscommunicatingprofessionally.Let'slearnaboutthisinfurtherdetail,ElectronicDataInterchange(EDI)

Electronic Data Interchange (EDI) is a computer-to-computer exchange of business documents in a standard electronicformatbetween two or more trading partners. It enables companies to exchange information electronically in a structuredformat,eliminating the need for manual data entry and reducing the cost and time associated with paper-based transactions.

EDI was first introduced in the 1960s as a way for companies to exchange business documents electronically. Over time,thestandardization of EDI formats and protocols has enabled businesses to integrate their internal systems with those of theirtradingpartners, improving efficiency and reducing errors.

EDItransactionscanincludepurchaseorders,invoices,shippingnotices,andotherbusinessdocuments.TheEDIstandarddefinestheformatand content of these documents, ensuring that they are easily interpreted by both the sender and the receiver.

EDI has become an important part of many businesses, particularly those in the supply chain and logistics industries. It allowsforfaster and more accurate processing of transactions, leading to improved customer satisfaction and increased profits.

Imagine writing a letter to your friend while communicating every time, Can not imagine right? Since today humans live in anerawhere they can very easily communicate through the internet. Now, imagine the same case with businesses, wherecommunicationand exchange of very important documents are constantly required, doing this the old way, it will take forever forthe messages toreach the other party, butalso the documentswill pile up as there is a lotofinformation that is needed tobe storedand kept. It is atedious and cumbersome process indeed, this is where EDI plays its role.

ElectronicDataExchangeisthedirectexchangeofdataandimportantbusinessdocumentsthroughtheInternetandinaveryprofessionalmanner.Twodifferentcompaniessittingattheextremecornersoftheworldcanveryeasilyinterchangeinformationordocuments(likesalesorders,shipping notices, invoices, etc) with the help of EDI.

EDIDocuments:
ThemostcommondocumentsexchangedviaEDIare:

- Invoices
- PurchaseOrders
- FinancialInformationletters
- TransactionBills
- Shippingrequestsandnotifications
- Acknowledgmentandfeedback
- Transcripts
- Claims
- BusinessCorrespondenceletters

EDIUsers:

- Centralandstategovernmentagencies
- Industry
- Banking
- Retailing
- Manufacturing
- Insurance
- Healthcare
- Automotive
- Electronics
- Grocery
- Transportation

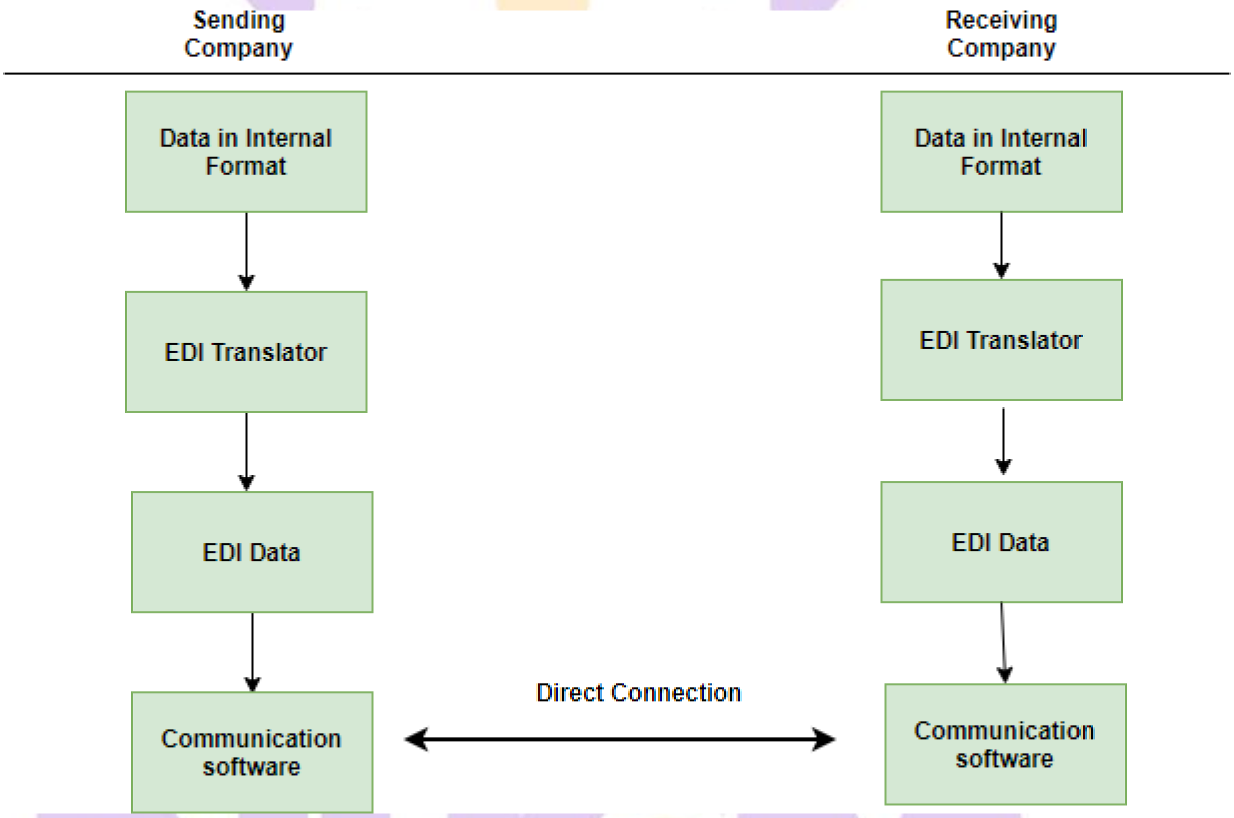
HistoryofEDI

EdwardGuilbertis knowntobethefatherofelectronicdataexchange,introducedEDIbackinthe1960sinthesupplychains.TheUS Transportation industry implemented EDI for better communication among differentcompanies. In 1985, the UN createdEDIFACTEDIforbetterreachofGlobaltechnology.Approximately12000companiesstartedusingEDIintheUS.TheUSgroceryandautomobileindustryvery swiftlyacceptedEDI dueto the easy process and standard form of data exchange. In today'stime,withfollowingEDI'scompliance, the big and major companies are using EDI for their communication among businesses.

ExamplesofEDIincludePurchaseorders,invoices,shippingstatuses,paymentinformation,andsoon.HowEDIworks

?

The data or the information that one company sends the other first gets prepared to be sent, then the information/documentistranslatedintoEDI format.Thedocumentisthenconnectedandtransmittedtotheotherbusiness,theconnectionisdirectandpointtopoint.



UsesofEDI:
EDIiswidelyusedinvariousindustriesforexchangingbusinessdocumentselectronically.SomeofthecommonusesofEDIare:

- **OrderProcessing:**EDI allowscompaniestoexchangepurchaseordersandsalesorderselectronically,eliminatingthe need for manual data entry and reducing errors.
- **Invoicing:**EDIcanbeusedtoexchangeinvoiceselectronically,reducingthetimeandcostassociatedwithpaper-basedinvoicing.
- **ShippingandReceiving:**EDIcanbeusedtoexchangeshippingnoticesandreceivingdocuments,enablingcompaniestotrack the movement of goods in real-time.
- **InventoryManagement:**EDIcanbeusedto exchangeinventoryinformation,enablingcompaniesto managetheirinventory levels more effectively.
- **SupplyChainManagement:**EDIisusedextensively inthesupplychainmanagementprocess,enablingcompaniestoexchange information with their suppliers, distributors, and customers.
- **Healthcare:**EDIisusedinthehealthcareindustrytoexchangepatientdata,claims, andotherhealthcare-relatedinformation between healthcare providers, insurance companies, and government agencies.
- **FinancialTransactions:**EDIcanbeusedtoexchangefinancialtransactionssuchaspaymentadviceand remittanceadvice, reducing the time and cost associated with manual payment processing.

AdvantagesofEDI:
ThereareseveraladvantagestoElectronicDataInterchange:

- **Thepaperusagereduced:**Theexpenseofstoring,printing,recycling,reducesupto themaximumamountduetotheEDI.
- **ImprovedqualityofData:**ThedataentryerrorsarereducedduetoEDI.

- **SpeedIncreases:**Thebestadvantageistheincreaseinthespeedofthe datainterchange.Witheverythinggoingonline, the speed of the information transfer increases exponentially.

- **Security:**ByfollowingtheProtocolsandthestandardrules, thesecurityofalltheimportantdocumentsisalwayssecure and safe.
- **Informationaccuracy:**Sincetheinformationexchangedisbasedonstandardsagreedbythesenderandreceiverboth, the correct information is always transferred regardless of where they belong to.
- **LessCost:**Withverylesserrors,fastresponsetime,everythingbecomingautomated, andnouseofpaper,thecostautomaticallyreduces.

DisadvantagesofEDI:

- TheinitialsetupoftheEDIisveryTime-consuming.
- EDIstandardskeeponchangingaftersomeamountoftime.
- AverysystematicandproperbackupisrequiredastheentiredatareliesonEDI.
- ThesetupandmaintenanceoftheEDIisveryExpensive.

CYBERSECURITYMARKETSIZE&SHAREANALYSIS-GROWTHTRENDS&FORECASTS(2023-2028):

The report covers Global Cybersecurity Market Growth and is Segmented by Product Type (Solutions (Application Security, Cloud Security, Consumer Security Software, Data Security, Identity and Access Management, Infrastructure Protection, IntegratedRiskManagement,NetworkSecurityEquipment),Services(Professional,Managed)),byDeployment(On-premise,Cloud), by End-user Industry (BFSI, Healthcare, Aerospace and Defense, IT and Telecommunication, Government, Retail, Manufacturing), by Geography (North America (United States, Canada), Europe (United Kingdom, Germany, France, Italy, Spain, Netherlands, Nordic Region, Poland, Russia), Asia-Pacific (China, South Korea, Japan, India, Singapore, Malaysia, Australia, Indonesia), and Rest of the World (Latin America (Brazil, Mexico, Colombia, Argentina), Middle East and Africa (GCC (Saudi Arabia, United Arab Emirates, Rest of GCC), Africa (South Africa, Egypt, Morocco))). The market sizes and forecasts are provided in terms of value in USD for all the above segment.

CybersecurityMarketSize:

StudyPeriod	2018-2028
BaseYearForEstimation	2022
CAGR	11.44%
FastestGrowingMarket	Asia-Pacific
LargestMarket	NorthAmerica
MarketConcentration	Low

CybersecurityMarketAnalysis

TheCybersecurityMarketsizeisestimatedatUSD182.86billionin2023,andisexpectedtoreachUSD314.28billionby2028,growingata CAGR of 11.44% during the forecast period.

Cybersecurity protects the network, information, and personal data from cyberattacks. The trends of BYOD, AI, IoT, and machinelearningincybersecurityarerapidlygrowing.Forinstance,machinelearningoffersadvantagesinoutlierdetection, which benefits cybersecurity.

- Thecybersecurityindustryecosystemcomprisesseveralregionalclustersofcybersecurityfirmscontributingtoglobal market dynamics. In the current market scenario, the cybersecurity industry operates in three distinct mega-clusters: the San Francisco Bay Area (SFBA), Metropolitan Washington, DC, and Israel.

- Thethreecybersecuritymega-clusterssharetwoessentialcharacteristics.Thefirstisthatthestartupandhigh-techinnovationcultureisasignificant growthdriverforallthreeecosystems.SFBAandIsrael havethriving startup ecosystems with a substantial associated flow of risk capital. They are heavily focused on products, while Washingtonexhibitsahigherproportion of service-basedfirms(in Washington, only11%of cybersecurity firmsarefocusedsolelyonproducts).Thesecondcharacteristicisthelinkbetweenhumancapitalandnational security.

- Ransomware attacks have ravaged many state and local public sector agencies. In some cases, entire local governmentswere forcedto declare an emergency due to massive leaksof sensitive data andlossof services. For instance, in June 2021, JBS Foods, the world's leading meatpacking enterprise, declaredthat it had paid a USD 11 million ransom to REvil ransomware threat actors following a cyberattack that forced the company to shut down production at several sitesworldwide, including its production facilities in United States, Australia, and Canada.

- Oneofthemajorcausesofgrowingcyberattacksisthelackofskilledcybersecuritypersonnelineachindustry. The number of experienced cybersecurity professionals, especially in Europe, Asia-Pacific, Latin America, and Middle-East are low compared to the need for security professionals to handle cyber threats for financial institutes, government organizations, and private sector/industrial businesses.

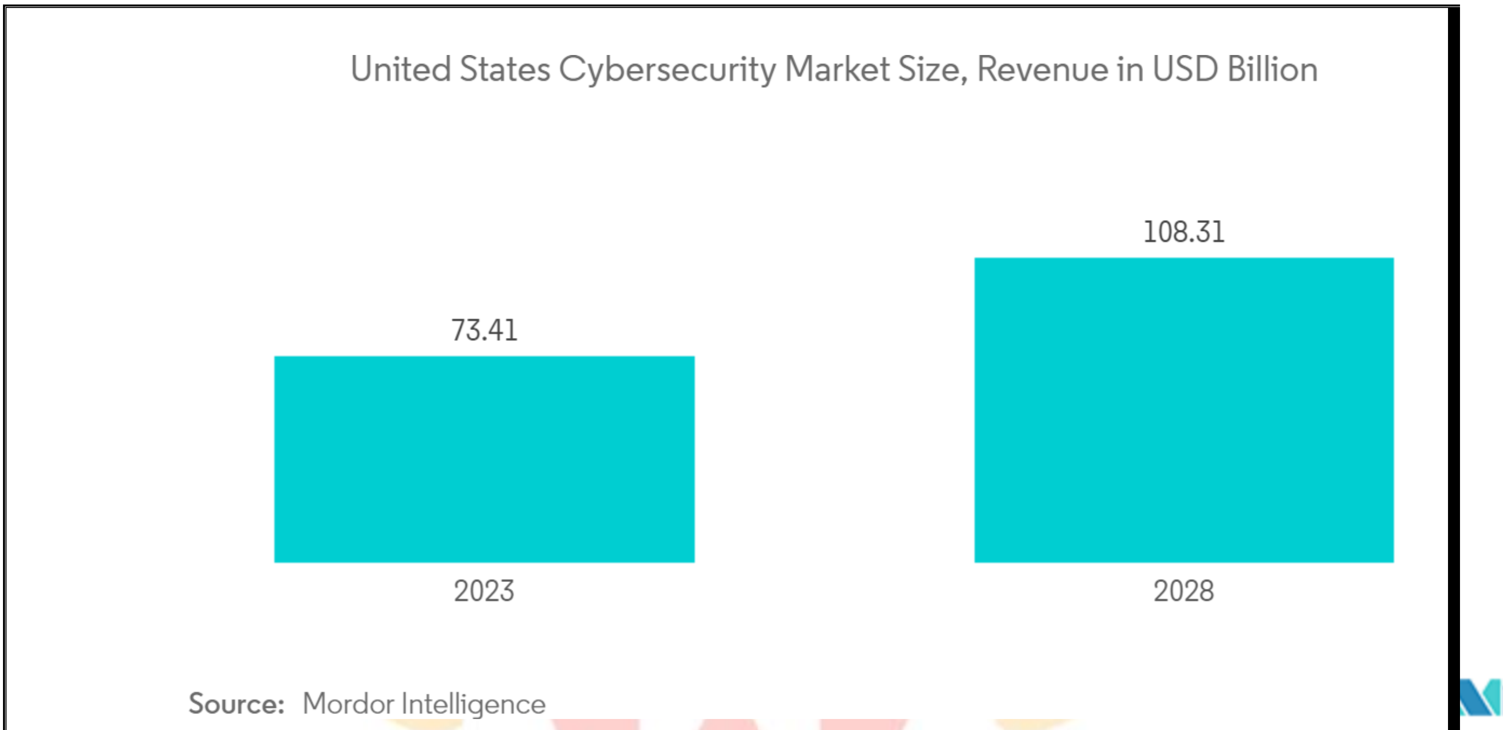
- Due to the ongoing COVID-19 pandemic, countries worldwide have implemented preventive measures. With schoolsbeingclosedandcommunitiesbeingaskedtostayat home,multiple organizationshave foundawayto enable their employees to work from their homes. This has, thus, resulting in a rise in the adoption of video communication platforms.

CybersecurityMarketStatistics

Cybersecurity Market growth is not evenly distributed across regions. The US, China, Germany, the UK, and Japan are the largest country markets for Cybersecurity, however, many smaller country market segments are expected to register much higher growth compared to these giants. For example, Japan is one of the top five Cybersecurity Markets but lags behind emerging economies such as India and Brazil in terms of future growth.

UnitedStatesCybersecurityMarketSize

ThecybersecuritymarketrevenueintheUnitedStateswasvaluedatUSD73.41billionin2023.ItisexpectedtoreachUSD 108.31 billion by 2028, growing at a CAGR of 8.09% during the forecast period (2023-2028). This can be attributed to the increasing frequencyandsophistication of cyber-attacksinthe country. Moreover, the growing regulatoryrequirement leads many organizations to adopt and invest in cybersecurity solutions, as many industries in the United States are subject to regulations, which require the organization to implement.



United States Cybersecurity Market Size, Revenue in USD Billion

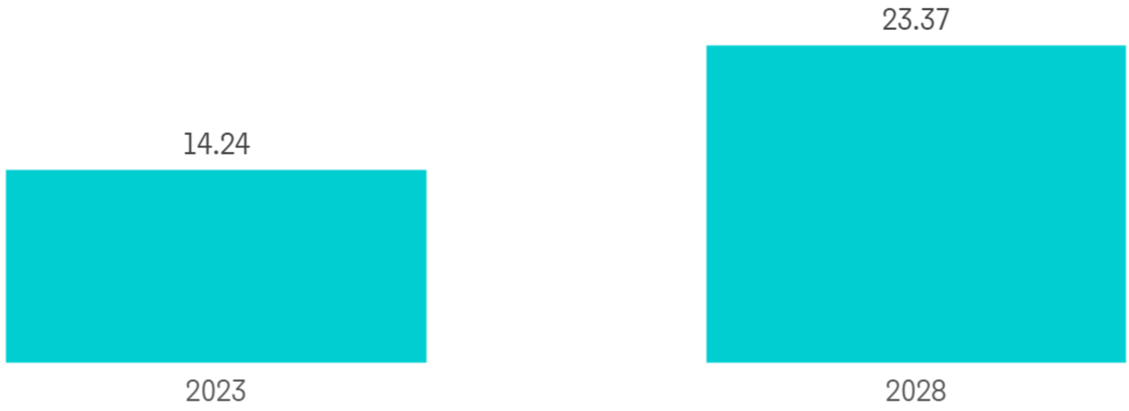
Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CAGR
UnitedStatesCybersecurityMarketSize	USD73.41billion	USD108.31billion	8.09%

UnitedKingdomCybersecurityMarketSize

ThecybersecurityservicesmarketsizeintheUnitedKingdomwasvaluedat USD14.24billionin2023.Itisexpectedtoreach USD23.37billionby2028,growingataCAGRof10.42%duringtheforecastperiod(2023-2028).Themarketisgrowingduetotheincreased rate of cybercrimes and the focus on developing new solutions to tackle them. With the growing 5G and total fiberbroadband networks in the country, the government, in collaboration with telecommunication companies, is takinginitiatives to tackle cyberattacks and improve security standards and practices across the UK telecom sector.

United Kingdom Cybersecurity Market Size, Revenue in USD Billion

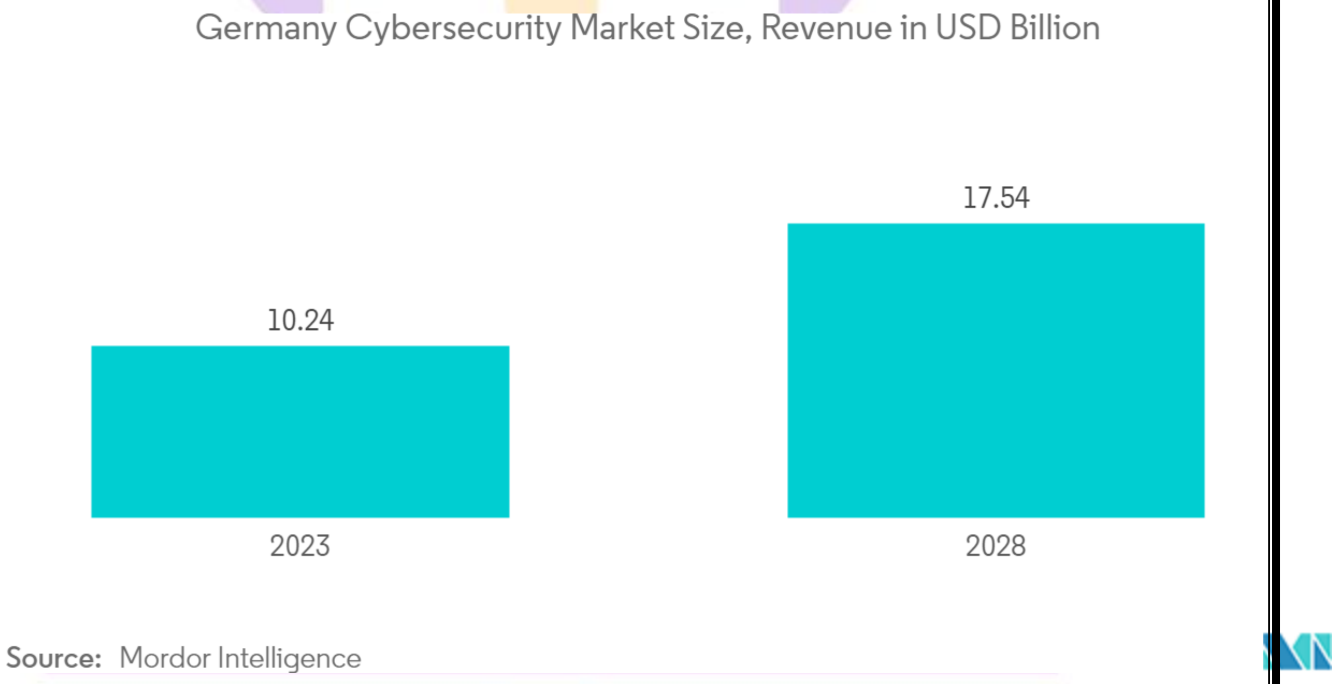


Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CAGR
UnitedKingdomCybersecurityMarketSize	USD14.24billion	USD23.37billion	10.42

GermanyCybersecurityMarketSize

ThecybersecuritymarketinGermanywasvaluedatUSD10.24billionin2023,anditisanticipatedtoreachavalueofUSD 17.54 billion by 2028, registering aCAGR of 11.36% during the forecasted period (2023-2028). Thisgrowth can be associated withthecountry’sstronganddiversifiedcybersecurityecosystem,awidespectrumofestablishedenterprises,startups, researchorganizations,anduniversitiesdedicatedtocybersecurity,andsupportivegovernmentpolicies,suchastheNational Cybersecurity Strategy and the Cybersecurity Act.


Germany Cybersecurity Market Size, Revenue in USD Billion

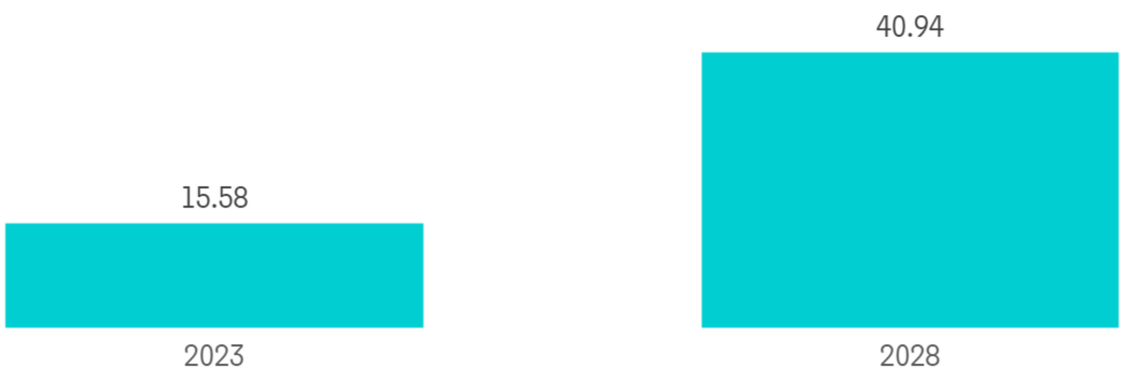
Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CAGR(2
GermanyCybersecurityMarketSize	USD10.24billion	USD17.54billion	11.36%

ChinaCybersecurityMarketSize

The cybersecurity market revenue in Chinawasvaluedat USD 15.58billion in 2023. It isexpectedto reach USD 40.94 billion by 2028, growing at a CAGR of 21.31% during the forecast period (2023-2028). The market growth can be attributed to increasing cyberattacks and the rising adoption of public cloud computing leading to more enterprises re-allocating their business systems to cloud platforms.

China Cybersecurity Market Size, Revenue in USD Billion



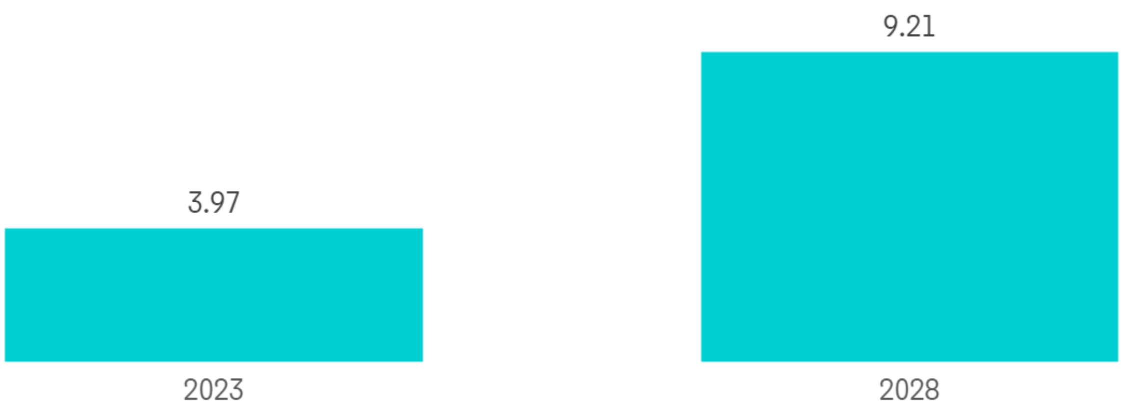
Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CGR(20
ChinaCybersecurityMarketSize	USD15.58billion	USD40.94billion	2.31%

IndiaCybersecurityMarketSize

The cybersecurity market revenue in Indiawasvalued at USD 3.97 billion in 2023. It isexpected to reach USD 9.21 billion by 2028, growing at a CAGR of 18.33% during the forecast period (2023-2028). An exponential rise in the exchange of personal dataand currency transactions due to digitalization initiatives has resulted in the need for resilient cybersecurity solutions and services in the country.

India Cybersecurity Market Size, Revenue in USD Billion

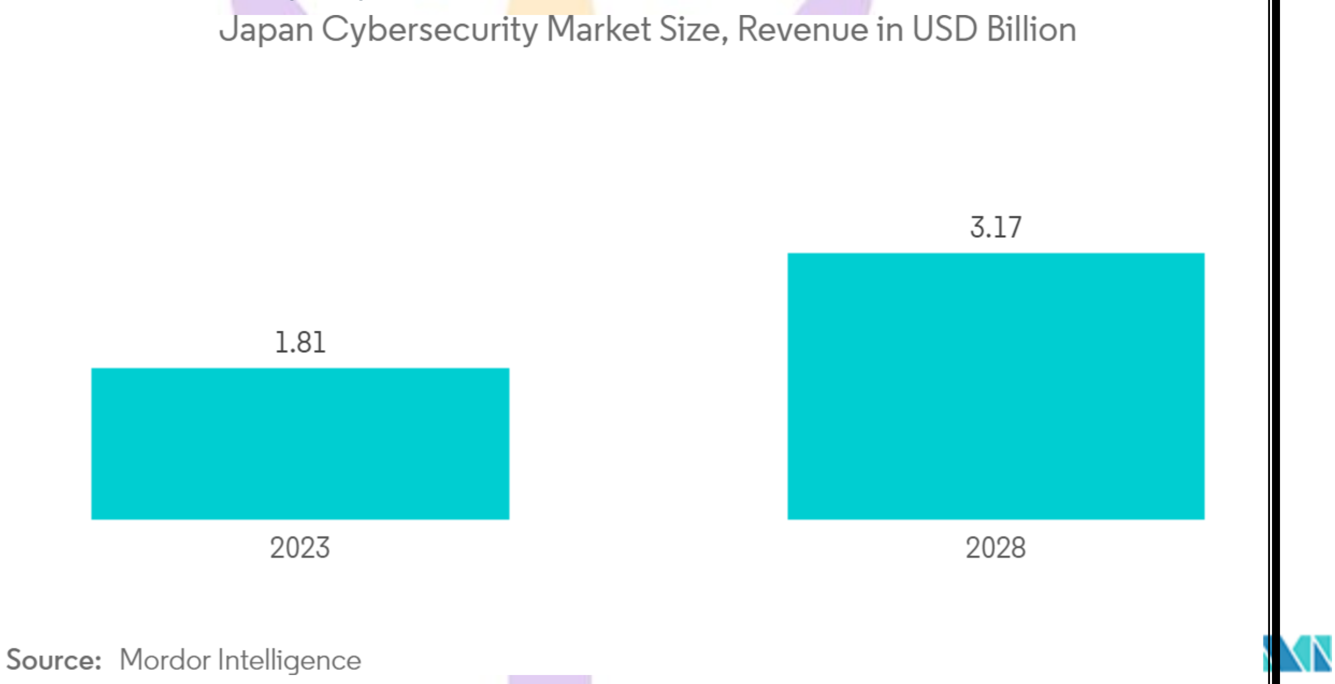


Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CAGR(20
IndiaCybersecurityMarketSize	USD3.97billion	USD9.21billion	18.33%

JapanCybersecurityMarketSize

ThecybersecuritymarketrevenueinJapanwasvaluedatUSD 1.81billionin2023.ItisexpectedtoreachUSD3.17billionby 2028,growing at a CAGR of 11.89% during the forecast period (2023-2028). The country's cybersecurity market is gaining interest from Japanese enterprises and the government at a rapid pace. The rise in cyberattacks on Japanese organizations prompts the government to establish new strategies, legislation, and facilities.

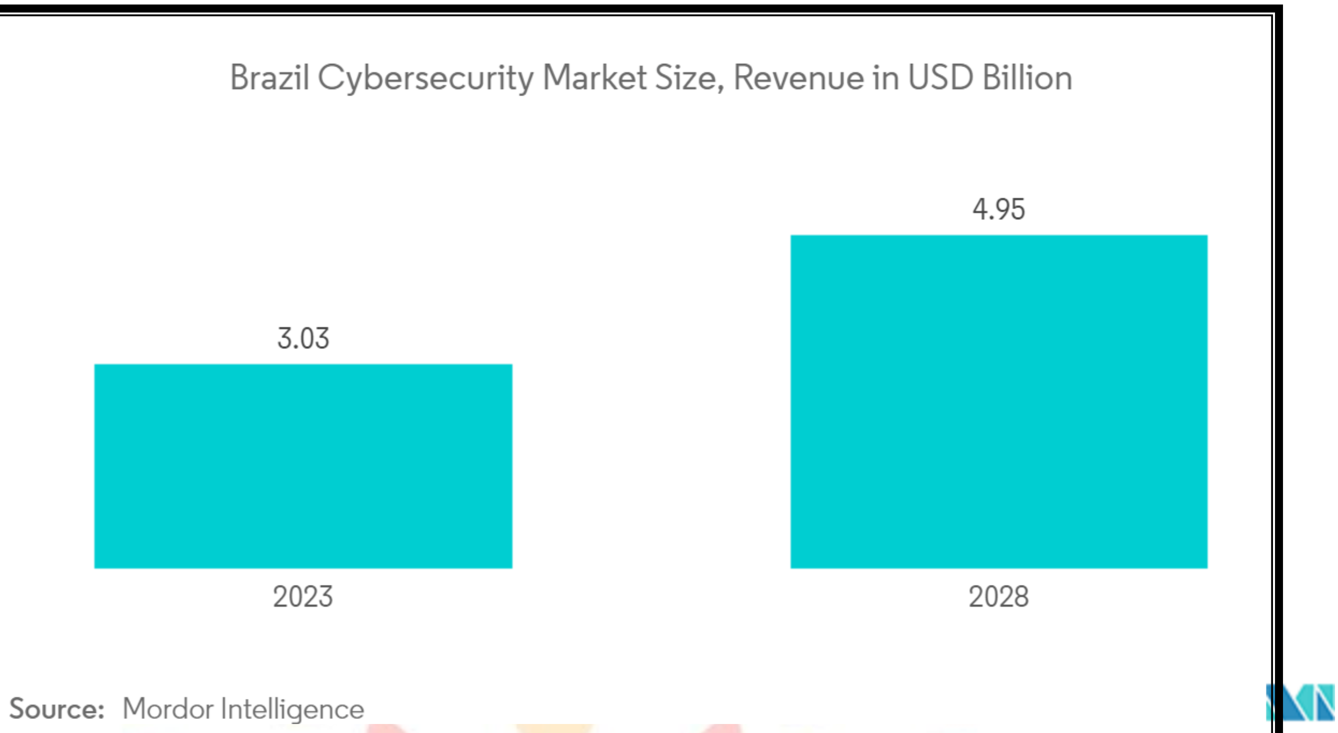

Japan Cybersecurity Market Size, Revenue in USD Billion

Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CAGR(20
JapanCybersecurityMarketSize	USD1.81billion	USD3.17billion	11.89%

BrazilCybersecurityMarketSize

The cybersecuritymarket revenue inBrazilwasvaluedat USD3.03billionin2023.It isexpectedtoreach USD4.95billionby 2028,growingataCAGRof10.30%duringtheforecastperiod(2023-2028).Themarketisbeingdrivenbyincreasinginvestments by Brazilian fintech and government interventions in improving the overall cybersecurity infrastructure.



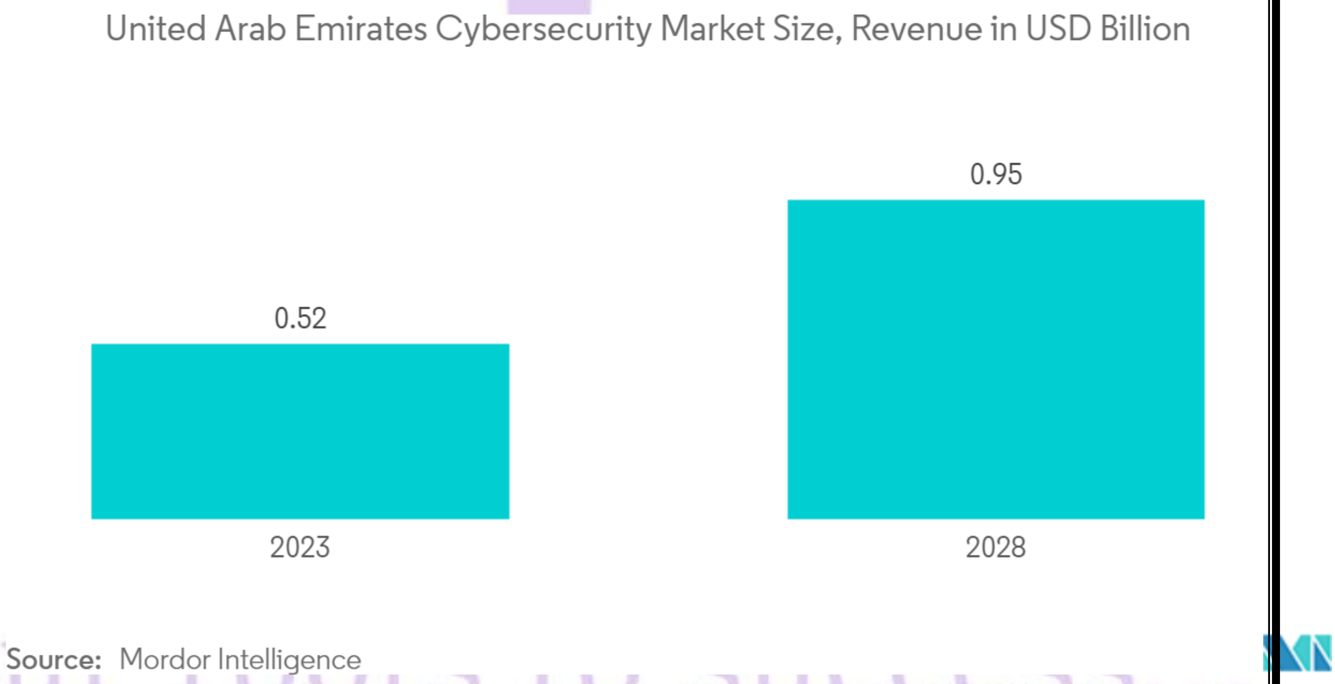
Brazil Cybersecurity Market Size, Revenue in USD Billion

Source: Mordor Intelligence

	2023MarketSize	2028MarketSize	CAGR(20
BrazilCybersecurityMarketSize	USD3.03billion	USD4.95billion	10.30%

UnitedArabEmiratesCybersecurityMarketSize

ThecybersecuritymarketrevenueintheUnitedArabEmirateswasvaluedatUSD0.52billionin2023.Itisexpectedtoreach USD 0.95 billion by 2028, growingat a CAGR of 12.72% during the forecast period(2023-2028). The market is being driven by an increasing focus on a digital economy, government initiatives, and increased interest from global and local vendors.



United Arab Emirates Cybersecurity Market Size, Revenue in USD Billion

Source: Mordor Intelligence

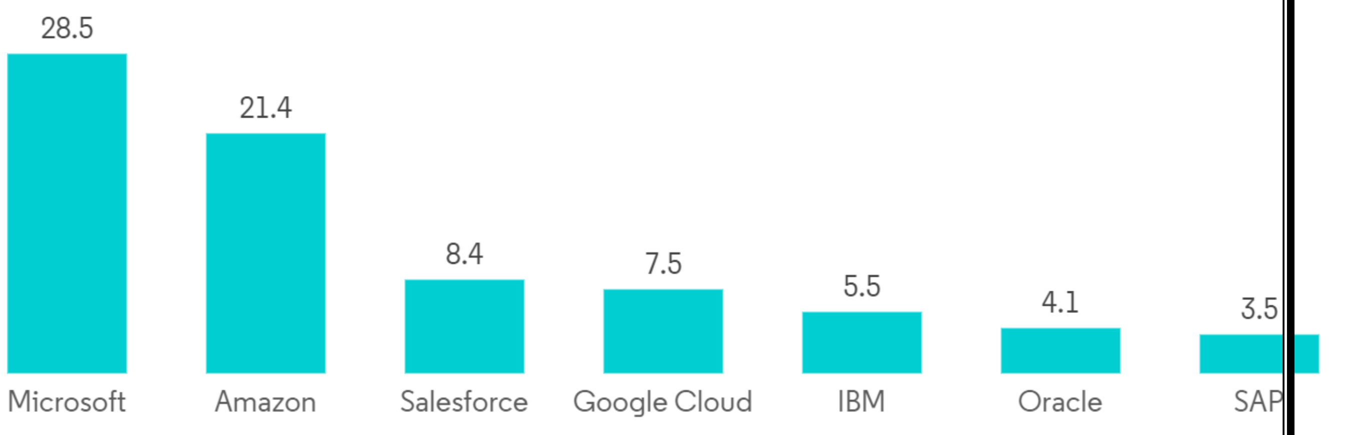
	2023MarketSize	2028MarketSize	CAG
UnitedArabEmiratesCybersecurityMarketSize	USD0.52billion	USD0.95billion	12.

Get10-yearmarketsizedatabysegmentsandin-depthanalysisonspecificcountries.Contactusnow.

CybersecurityMarketTrends

TheCloudSegmenttoWitnessSignificantGrowth

- The increasing realization among enterprises about the importance of saving money and resources by moving theirdatatothecloudinsteadofbuildingandmaintainingnewdatastoragedrivesthedemandforcloud-based solutions. Owing to multiple benefits, cloud platforms andecosystems are anticipated to serve as a launchpad for the explosion in the pace and scale of digital innovation over the next few years.
- Cloud-basedsolutionsalsobenefitfromlowercapitalexpenditurerequirements,makingthemmuchmore compelling.Deployingcloud-basedservicescansignificantlyreducetheCapexrequirementsascompaniesneed notinvestinhardwarecomponents.Cloudsolutionsalsoenablebetterpredictionofthecostofanapplication, andcompaniesdon'tincurmuchupfrontcosttoincorporatethetechnology.Also,thehardwareandITsupportsavings make cloud-based solutions much more affordable.
- Companiesthatareconsideringmovingfromon-premisesoftwaretocloud-basedsolutionsareprimarily checking the potential solutions for their key security features, including standards compliance and intrusion preventionanddetection.
- In October 2022, Google Cloud declared a significant expansion of its trusted cloud ecosystem. It highlighted newintegrationsandofferingswithmore than twentypartners,focusingonenablinggreaterdatasovereignty controls,supportingZeroTrustmodels,unifyingidentitymanagement,andimprovingendpointsecurity forglobal businesses.
- Cloudtechnologyprovidesorganizationswiththeflexibilitytheyneedtoincreaseanddecreasetheirbandwidth withtheneedsoftheiroperations.Thisapproachcancutcostsandgivebusinessesanedgeoverthecompetition.



Top-10 Cloud Vendors, by Revenue, in USD Billions, Global, 2023

Source: cloudwars.co

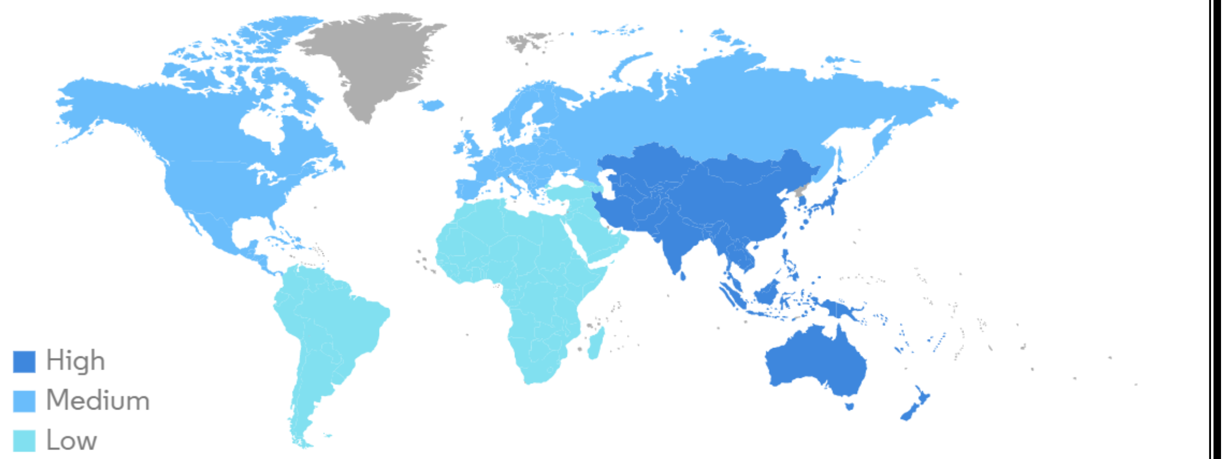
Tounderstandkeytrends,DownloadSampleReport

NorthAmericaisExpectedtoHoldMajorMarketShare

- Cybersecurityhasbecomeanincreasinglyimportant areaoffocusinthe UnitedStatesinrecentyearsdue to thegrowingnumberofcyberthreatsandattacksthatorganizationsandindividualsface.Accordingtothe IdentityTheftResourceCenter,thenumberofdatacompromisesandindividualsimpactedintheUnitedStatesin2022 was1,802and422.14million,respectively.
- Theincreasingfrequencyandsophisticationofcyber-attacksaredrivingtheadoptionofcybersecuritysolutions intheUnitedStates.Moreover,thegrowingregulatoryrequirementleadsmanyorganizationstoadoptand investincybersecuritysolutions,asmanyindustriesintheUnitedStatesaresubjectto regulationssuchasHIPPA, GDPR, and PCI DSS.
- Education,thepublicsector,universities,healthcare,andmunicipalitieswereamongthemajorsectorsaffected bycyber-attacksintermsofdatabreachesandransomwareintheUnitedStatesin2022.Therehasbeen significant investment in cybersecurity research and development in the United States. The United States government isallocating alargenumberof funds. Forinstance, inApril 2022,the UnitedStatesDepartmentofEnergy (DOE) announced that it would invest USD 12 million in six new research, development, and demonstration (RD&D) projects to develop innovative cybersecurity technology to ensure that energy delivery systems are designed, installed, operated, and maintained to survive and recover quickly from cyberattacks.
- In Canada, cybercrime is rapidly gaining traction, and the impact is increasing alarmingly. According to the MinistryforGovernmentDigitalTransformation,Quebec,around3,992provincialgovernmentwebsites, includingthoserelatedtohealth, education, andpublicadministration,canbeatrisk.

- Inorderto supportthedevelopmentofastrongnationalcybersecurityecosystem,the MinisterofInnovation, ScienceandIndustryannouncedthattheNationalCybersecurityConsortium(NCC)receiveduptoUSD80million toleadtheCyberSecurityInnovationNetwork(CSIN)inFebruary2022.Thisfundingwascrucialtofostera strongnationalcybersecurityecosysteminCanadaandpositionthecountryasagloballeaderincybersecurity.

Cybersecurity Market - Growth Rate by Region



Source: Mordor Intelligence

Tounderstandgeographytrends,DownloadSampleReport

CybersecurityIndustryOverview

Thecybersecuritymarketcomprisesseveralglobalandregionalplayersvyingforattentioninafairlycontestedmarketspace.Although the market poses high barriers to entry for new players, several new entrants have been able to gain traction. Crowdstrike Holdings Inc., Check Point Software Technologies Ltd, Cisco Systems Inc., Cyberark Software Ltd, and Dell Technologies Inc. are major players in the market.

- InFebruary2023,CheckPointSoftwareTechnologiesLtdannouncedtheintroductionofCheckPointHorizon XDR/XPR, a cooperative cybersecurity solution. It effectively protects organizations against developing cyber threatsbysmartlycorrelatingdataandtryingtothwartattacksacrossallvectors,reducingtheimpactofthreats and making it simple for supervisors and analysts to comprehend and respond to incidents.
- InDecember2022,CrowdStrikeannouncedthedevelopmentoftheCrowdStrikeFalconplatformtogivethe sector'sfinestadversary-drivenexternalattacksurfacemanagement(EASM)solutionforbetteradversary intelligenceandreal-timeinternetaccessdetection.CrowdStrikeFalconSurface,astandalonemodulefeaturingabilities from the recent acquisition of Reposify, was announced as part of the platform update.

CybersecurityMarketLeaders

1. CrowdStrikeHoldings,Inc.

2. CheckPointSoftwareTechnologiesLtd

3. CiscoSystemsInc.

4. CyberArkSoftwareLtd

5. DellTechnologiesInc.

CybersecurityMarketNews

- InMarch2023,CrowdStrikeandDellTechnologiesannouncedanewpartnershipagreementtoprovide enterprises with seamless and affordable products to help them avoid, detect, and respond to cyber-attacks. Thepartnershipincludesfocusedservicesforcompaniesofallsizes.Duetothenewstrategicalliance, organizations can manage cyber threats and safeguard their cloud workloads, endpoints, identities, and data.

- InMarch2023,InfinityGlobalServices,acomprehensivesecuritysolutionthatcanenablebusinessesofallsizes toprotecttheirsystems,fromthecloudtothenetworktotheendpoint,waspresentedbyCheckPointSoftware Technologies Ltd. The new service is expected to increase Check Point's end-to-end security offerings across thirty categories, enabling businesses to develop and improve their cybersecurity procedures and systems and show their level of cyber resilience.

CybersecurityMarketReport-TableofContents

EmergingTrendsinCybersecurity:

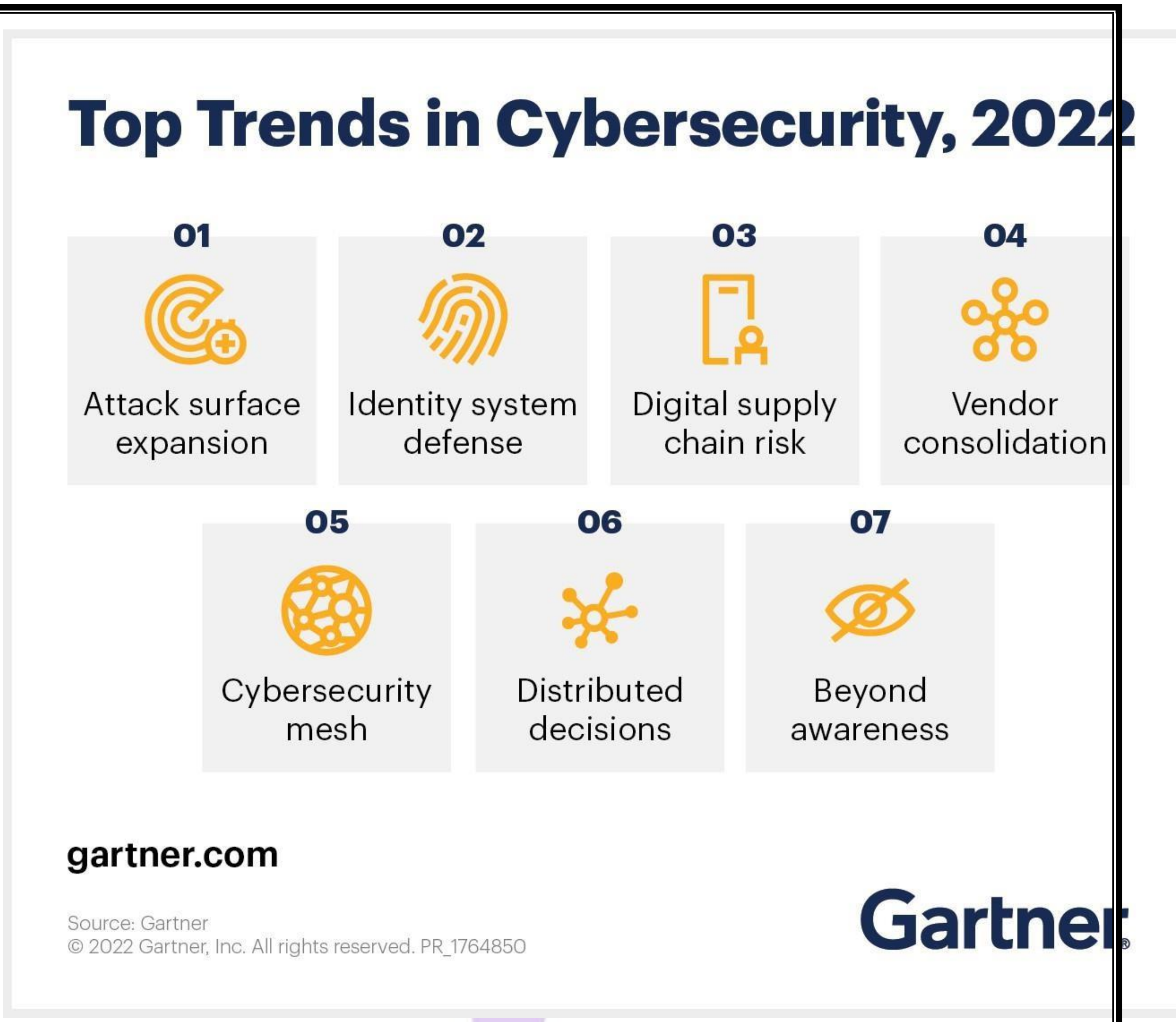
Theever-expandingdigitalfootprintofmodernorganizationsdrivesthisyear'stopcybersecuritytrends.

Securityandriskexecutivesfaceacriticaljuncture,asthedigitalfootprintoforganizationsexpandsandcentralizedcybersecurity control becomes obsolete.

Hybridworkanddigitalbusinessprocessesinthecloudhaveintroducednewrisks.Atthesametime, sophisticated**ransomware**,attacksonthe**digitalsupplychain**anddeeplyembeddedvulnerabilitieshaveexposed technologygapsandskillsshortages.

"Thesedisruptions don'texistinisolation;theyhaveacompoundeffect,"says PeterFirstbrook,VPAnalystatGartner."To addresstherisks,CISOs needto **transitiontheirroles**fromtechnologists whopreventbreachestocorporatestrategistswho managecyberrisk."

Thosewhounderstandtheseseventrendswillbebetterabletoaddressnewrisksandelevatetheirrole,butitrequiresreframingthe security practice and rethinking technology, as well as preparing to respond to new threats.



Top Trends in Cybersecurity, 2022

01 Attack surface expansion

02 Identity system defense

03 Digital supply chain risk

04 Vendor consolidation

05 Cybersecurity mesh

06 Distributed decisions

07 Beyond awareness

gartner.com

Source: Gartner
© 2022 Gartner, Inc. All rights reserved. PR_1764850

Gartner

TrendNo.1:Attacksurfaceexpansion

Currently,60%ofknowledgeworkersareremote,andatleast18%willnotreturntotheoffice.Thesechangesinthewaywework, together with greater use of public cloud, highly connected supply chains and use of **cyber-physical systems**have exposednewandchallengingattack“surfaces.”

Thisleavesorganizationsmorevulnerabletoattack.Gartnerrecommendssecurityleaderslookbeyondtraditionalapproachesto security monitoring, detection and response to manage a wider set of risks.

TrendNo.2:Identitysystemdefense

Identitysystemsarecomingundersustainedattack.Misuseof**credentials**isnowaprimarymethodthatattackersuseto accesssystemsandachievetheirgoals.Forexample,inthe**SolarWindsbreach**attackersusedasupplier'sprivilegedaccess toinfiltratethetargetnetwork.

Gartnerusesthetermidentitythreatdetectionandresponse(ITDR)todescribeacollectionoftools andprocessestodefend identity systems. In the longer term, more consolidated solutions will emerge.

TrendNo.3:Digitalsupplychainrisk

Gartnerpredictsthatby2025,45%oforganizationsworldwidewillhaveexperiencedattacksontheirsoftwaresupplychains,athree- fold increase from 2021.

Securityandriskmanagementleadersneedtopartnerwithotherdepartmentstoprioritize**digitalsupplychainrisk**andput pressureonsupplierstodemonstratesecuritybestpractices.

TrendNo.4:Vendorconsolidation

Securityproductsareconverging.Vendorsareconsolidatingsecurityfunctionsintosingleplatformsandintroducingpricingand licensing options to make packaged solutions more attractive.

Whileitmayintroducenewchallengessuchasreducednegotiatingpowerandpotentialsinglepointsof failure, Gartnersees consolidation as awelcometrendthatshouldreducecomplexity,cutcosts andimproveefficiency,leadingtobetteroverall security.

TrendNo.5:Cybersecuritymesh

The**cybersecuritymesh**isamodernconceptualapproachtosecurityarchitecturethatenablesthedistributedenterpriseto deployandintegratesecuritytoassets,whetherthey'reonpremises,indatacentersorinthecloud.

Gartnerpredictsthatby2024,organizationsadoptingacybersecuritymesharchitecturewillreducethefinancialimpactof individual security incidents by an average of 90%.

TrendNo.6:Distributeddecisions

Executiveleaders needafastandagilecybersecurityfunctiontosupportdigitalbusiness priorities.However,asmoreaspects of the business aredigitalized,thejobisbecomingtoobigforacentralizedCISOrole.Leading organizations arebuildingtheoffice of the CISO to enable distributed cyber judgment.

TheCISOandthecentralizedfunctionwillcontinuetosetpolicy,whilecybersecurityleadersareplacedindifferentpartsofthe organization to decentralize security decisions.

TrendNo.7:Beyondawareness

Humanerrorcontinuestofeatureinmostdatabreaches,showingthattraditionalapproachesto**securityawareness training**areineffective.Progressiveorganizationsaremovingbeyondoutdatedcompliance-basedawarenesscampaignsand investinginholisticbehaviorandculturechangeprogramsdesignedtoprovokemoresecurewaysofworking.

Inshort:

- Rethinkthesecuritytechnologystacktoaddresssophisticatednewthreats.
- Pushcybersecuritydecisionmakingouttothebusinessunitstoimproveyoursecurityposture.
- Evolveandreframethesecuritypracticetobettermanagecyberrisk.

UNIT-5

CaseStudyOnCyberCrimes
Harassment Via E-Mails:

HowToStopHarassingEmails:

You open your inbox, andthereit is again. Another email from your harasser. Whether it’s an ex-partner, adisgruntled customer,orsomeoneyou’veneverevenmet,harassmentviaemailisarealproblemthatcanhaveaseriousimpactonyour emotional well-being. So, you must be wondering, “how do I stop harassing emails” read on to find out.

TableofContents:

WhatisEmailHarassment?

Emailharassmentisatypeofonlineharassmentthatinvolvessendingunwanted,threatening,oroffensiveemailstosomeoneelse.This type of harassment canbeparticularly difficultto deal with becauseit can behard toknowwhothe harasseris and where they are located. Additionally, email harassment can be very upsetting and causethe victim a great deal of stress.

IsSendingHarassingEmailsaCrime?

Yes, emailharassment is atype of cybercrime and it is considered a form of cyberstalking.Depending on theseverityof the harassmentsomeonewhoactsonemailharassmentcanbechargedwithamisdemeanorwhichcarriesjailtime(oftenuptoa year), and fines, or a felony that carries up to 5 or even 10 years of prison time.

HowToStopHarassingEmails

1. Blockthesender'semailaddress.Thiswillstopthemfrom beingabletoemailyoudirectly.TodothisinGmail, click thethreedotsnexttothesender'snameandselect"Block."InOutlook,clickthe"…"nexttothesender'sname and select "Block."
2. Reporttheabusetoyour emailserviceprovider.If you'reusingGmail,youcanreportabusebyclickingthe three dots next to thesender's name and selecting "Report spam." In Outlook, click the "…" next to the sender's nameandselect"Reportas junk."Doingthiswillhelppreventfutureabusebyflaggingthesenderas a spammer.
3. Createafilter.Afilter is asetofrules thattells your emailservicehowtohandlecertaintypes of emails.For example,youcancreateafilterthatautomaticallydeletesallemailsfrom aparticularsenderorthatmoves all emails with certain keywords to a specific folder. Tocreate a filter in Gmail, click the three dots next to the

sender'snameandselect"Filtermessageslikethese."InOutlook,clickthe"…"nexttothesender'snameandselect "Createrule."

4. Setuptwo-factorauthentication.Two-factor authenticationis anextralayerofsecuritythatrequires youtoentera code in additiontoyour password when logging in to your email account. This makes itmuch moredifficult for someonetohackintoyouraccountandsendharassingemailsinyourname.Tosetuptwo-factorauthenticationinGmail, go to your account settings and select "Security." In Outlook, go to your account settings and select "Advanced securitysettings."
5. Keep evidence of theabuse. If you decidetotakelegal action against your abuser, havingdocumentation of theharassmentcanbehelpful.Saveanyabusiveemails youreceive inasafeplacesothatyoucanaccess them ifneeded.Youshouldalsokeeptrack ofanyothercommunications youhavewithyourabuser,suchas text messages or socialmediaposts. Keeping track of this information can betime-consuming, but it may be helpful if you decide to pursue legal action against your abuser down the road.

EmailSpoofing(OnlineAMethodOfSendingE-MailUsingAFalseNameOrE-MailAddressToMakeItAppearThatTheE-MailComesFromSomebodyOtherThanTheTrueSender:

Whatisemailspoofing?Acompleteguide

- ClareStouffer
- August31,20234minread

Haveyoueverreadanemailandwonderedifittrulycamefromthelistedsender?Ifso,itmaybeemailspoofing.To learnmoreaboutemailspoofing,followthisguide.

Emailspoofingdefinition

Emailspoofingisapracticeusedinscamsandphishingattackstodeceivepeopleintobelievingthemessagecame fromaknownortrustedsource.

Have youeveropenedanemailfromsomeoneyouknowonlytobeunsureifitwasthemwhowrotethemessage?

Whetheritseemslikea**spamemail**ortheyaskedyouapersonalquestiontheyalreadyknowtheanswerto,it'spossiblethesender maynotbewhotheyappeartobe.

How,youask?Theanswerisemailspoofing.

Email Spoofing Explained

Email spoofing is a practice used in scams and phishing attacks to **deceive people into believing the message came from a known or trusted source.**

Emailspoofingisapracticeusedinscamsand**phishingattacks**todeceivepeopleintobelievingthemessagecamefromaknownor trustedsource.**Cybercriminals**usethistechniquehopingthattherecipientwillnotnoticeandengagewiththemessageasifit'sa legitimateemail.

Butbeforeyoustartsecond-guessingevery email you'veeverreceived,readthroughthis completeguidewherewe'll coverhow email spoofingworks,whatitlookslike,andhowyoucanprotectyourselffromit.

Howdoesemailspoofingwork?+3typesofemailspoofs

Insimpleterms,thegoalofemailspoofingistomaketherecipientbelievetheemailiscomingfromsomeonetheycantrust.Then the attackerexploitsthattrust,whethertheyuseitforphishing,spreadingdifferent**typesofmalware**,ortarnishingthesender's reputation.Tohelpyouunderstandhowemailspoofingworks,herearethreedifferentwaysanemailspoofermaytrytotrickyou.

Displaynamespoofing

Displaynamespoofingisanexampleofspoofingemailheaderswhereonlythesender’s displaynameisfalsified.Withthis typeof emailspoofing,theemailaddressitselfwillnotmatchthedisplaynameattachedtotheemail.Forexample,youmaygetanemailthatsaysitis comingfromyourboss,butafteropeningthemessage,younoticethatthesender’s emailaddressdoes notmatchyour boss’s.

Thisispossibleifacybercriminalcreatesanewemailaddressunderyourboss’sname.Becausetheemailitselfislegitimate,thistype ofspoofedemailmightbypassanyspamfilters,thereforeeasilymakingitintoyourinbox.

Legitimatedomainspoofing

Legitimatedomainspoofingis amuchmorebelievableemailspoofingexample.Inthis case,boththedisplaynameandthesender’s addresswillbefake.CybercriminalscandothisbytakingadvantageofSimpleMailTransferProtocol(SMTP),whichisanemailprotocolusedfor sending messages.

Duringnormalemailcommunications,youremailclient(Gmail,Outlook,etc.)willautomaticallyenterthesender’saddresswheneveran emailissent.Intheeventofemailspoofing,theattackercanmanipulatethisinformation,makingitseemasiftheemailiscomingfrom someoneelse.BecauseSMTPdoes notprovideawaytoauthenticateemailaddresses,thescammercanmanuallychangethe“To,” “From,”and“ReplyTo”fieldswhensendingspoofingemails.

Look-alikedomainspoofing

Anotherexampleof emailspoofingistheuseoflook-alike domains.Anexampleof aspoofeddomainis"amaz0n.com."Inthis specificscenario,thespoofercreatedadomainattemptingtoimpersonate"amazon.com."Atfirstglance,youmaynotnoticethatthe "o"hasbeenreplacedwitha"0."

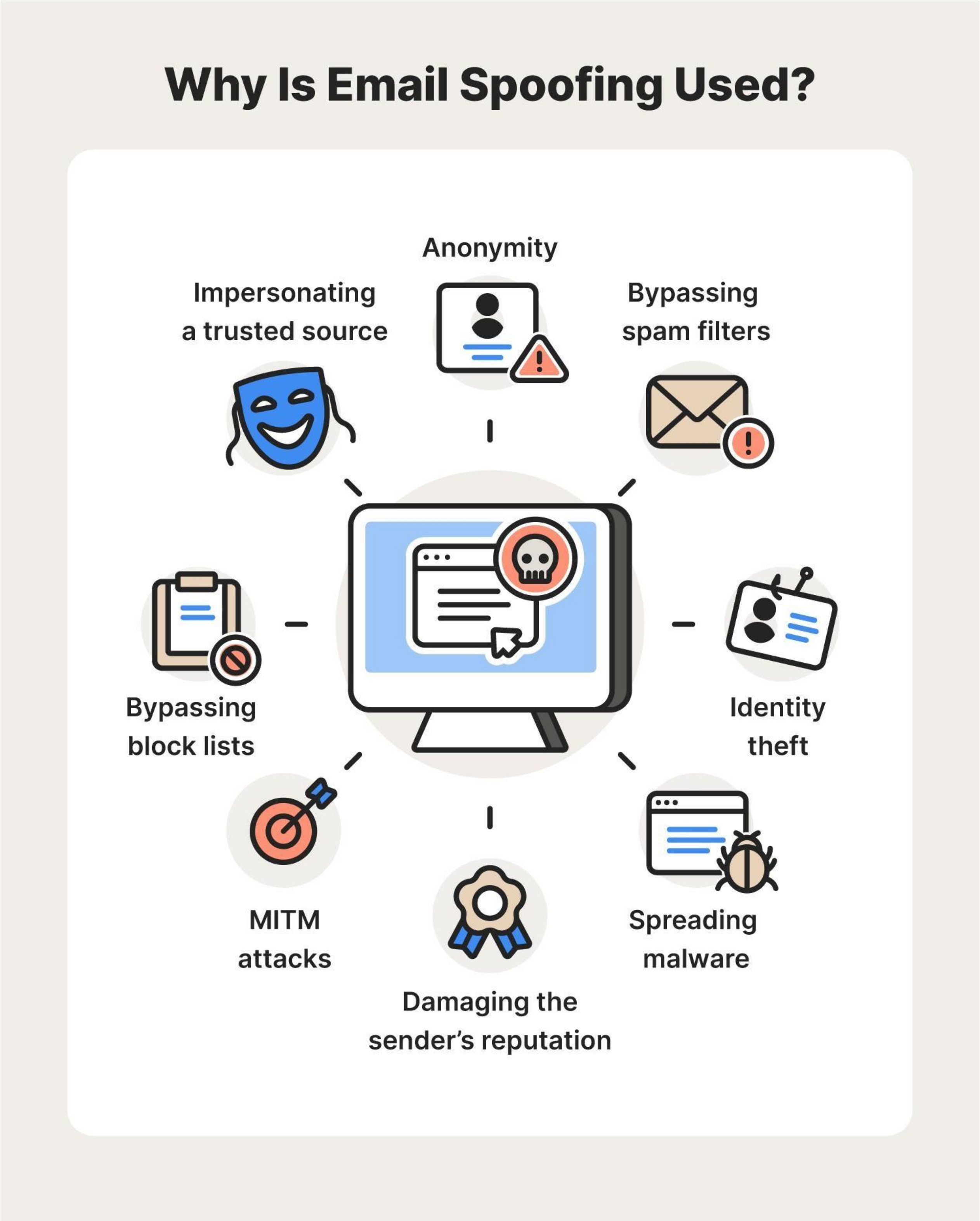
Thistechniquecanbeeffectiveifyoudon'tpaycloseattentiontothespoofedemailheader,especiallyifthecontentsoftheemail looklegitimate.Becauseofthis,it'simportanttoalwayspaycloseattentiontothesender'sdetailsbeforeengagingwithanemail.

Plus:What'sthedifferencebetweenemailspoofingvs.phishing?

Atfirstglance,emailspoofingmaysoundalotlikephishing,andinsomecases,thetwodoinvolveeachother.Butthesetwo cybersecuritythreatsaredifferent.Phishingisanothertypeof**cyberattack**utilizedbycybercriminalstotryandluresensitive informationfromyou.Thiscantakeplaceovertext,email,socialmedia,oronthephone(anattackalsoknownas**vishing**).

Nomatterwherethisattacktakesplace,themaingoalof phishingistoaccess yourpersonalinformationforfraudulentactivities suchas**identitytheft**.Emailaddressspoofingmayplayacrucialroleintheseattacks,allowingthecybercriminaltoappearasifthey aresomebodyelse.

Butphishingisn'ttheonlyreasonacybercriminalmayuseemailspoofingtotheiradvantage.Let'slookatsomeotherreasonsfor emailspoofing.



Why Is Email Spoofing Used?

Anonymity

Impersonating a trusted source

Bypassing spam filters

Bypassing block lists

Identity theft

MITM attacks

Spreading malware

Damaging the sender's reputation

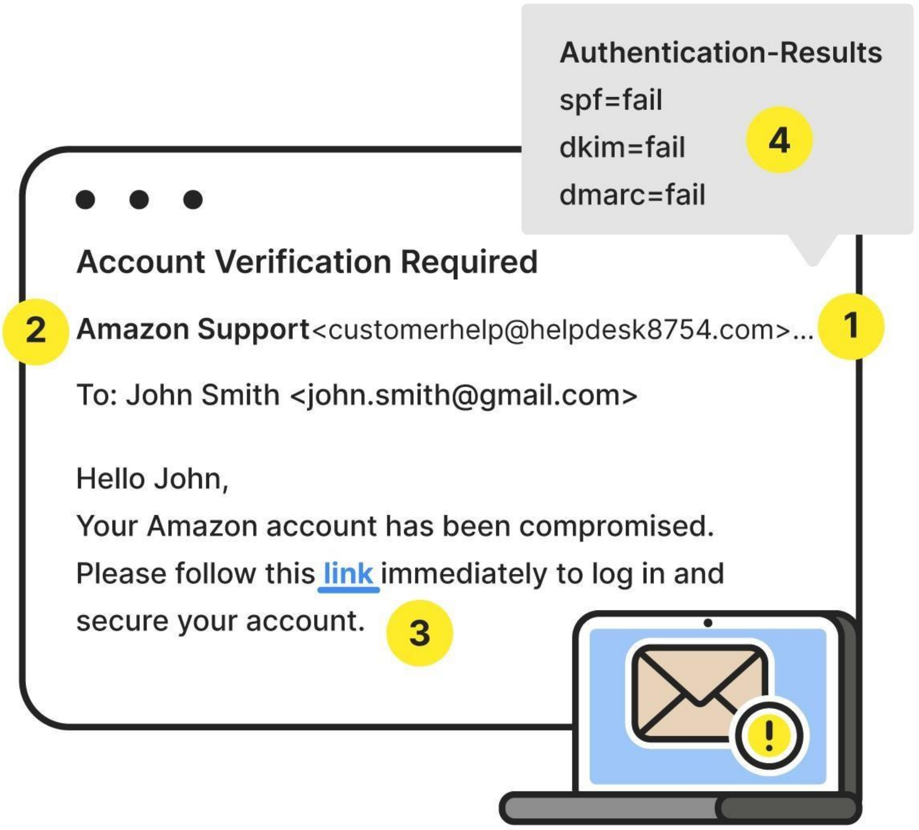
Reasonsforemailspoofing

Whileemailspoofingisoftenusedforphishingattacks,therearemanyotherreasonsacybercriminalmighttryspoofinganemail address,including:

- **Anonymity**: Email spoofingcanhelpconceal thesender'sidentity,allowingthemtocarryout attackswithoutfearof therecipientknowingwhotheytrulyare.
- **Bypassingspamfilters**:Mostemailprovidershavebuilt-inspamfiltersthatcanhelpfilteroutalotofspamemails.By utilizingemailspoofing,anattackermaybeabletosneakintoyourinbox.
- **Impersonatingatrustedindividualororganization**:Similarto**catfishing**,emailspoofingmaybeusedto impersonatesomeoneyouknow oratrustedorganizationinhopesthatyou'll disclosepersonal informationtheywouldn't be able to access otherwise.
- **Identitytheft**:Somespoofedemailmessagesaredesignedtotrickyouintogivinguplogincredentialsorother personalidentifyinginformation,whichcouldleadtoidentitytheft.
- **Bypassingblocklists**:Likebypassingspamfilters,emailspoofingmaybeusedtosendaspoofedemailtoa recipientwhotheywouldotherwisebeblockedfromcommunicatingwith.
- **Spreadingmalware**:Aspoofemailmaycontainmaliciouslinkswith**malware**,whichcoulddamageyourdeviceand putyourcybersecurityatrisk.
- **Man-in-the-middle(MITM)attacks**:Insomecases,emailspoofingisusedtocarryoutMITMattacks,whichalso involvephishing.Acommonexampleofthisiswhenanattackerimpersonatesyourbankusingafakesenderemailaddress and website link.
- **Damagingthesender'sreputation**:Becauseaspoofedmessagelookslikeit'scomingfromsomeoneelse,a cybercriminalcouldusethemessagetotarnishthesender'sreputationbysendingliesorrudemessages.

Asyoucansee,therearemanyreasonswhyacybercriminalmightuseemailspoofingtotheiradvantage.Buthowdoesemailspoofing work?Howtospotaspoofedemail.

What Does a Spoofed Email Look Like?



Authentication-Results
spf=fail
dkim=fail
dmarc=fail

Account Verification Required

Amazon Support<customerhelp@helpdesk8754.com>...

To: John Smith <john.smith@gmail.com>

Hello John,
Your Amazon account has been compromised.
Please follow this link immediately to log in and
secure your account.

1. Suspicious email address
2. Display name doesn't match address
3. Sense of urgency
4. Fails security protocols

Nowthatyouknowthedifferentwaysanemailspoofercouldtrytoimpersonateanothersender,youmaybewonderinghowyoucan quickly spot a spoofed email.

Wheneveryoucomeacrossanemailyou'reunsureabout,keepaneyeoutforthesewarningsigns.

- **Suspiciousemailaddress**:Besuretocheckandmakesurethattheemaildomainmatchesthecorrectdomainof whomeverthesenderisclaimingtobe.Also,keepacloseeyeoutfortyposorlook-alikedomains.
- **Displaynamedoesn'tmatchaddress**:Anotherhintofaspoofedemailmessageisifthedisplaynamediffersfromthe sender'semailaddress.Ifit'ssomeoneyou'vespokenwithbefore,checkandseeifthecurrentsender'saddress matchestheoneusedinpreviouscommunications.
- **Senseofurgency**:Becausespoofedemailsareoftenusedforphishingorothertypesofcyberattacks,thesendermayuse **socialengineering**tacticstocreateasenseofurgency,rushingyoutorespondorfollow theirinstructions.

Whileit's possiblethatnoteveryspoofingemailwillshow thesesigns,carefullyanalyzingthesender's addressanddisplaynamecan helpyoucatchsomespoofedemailsthatmayhavemadeittoyourinbox.Fortunately,mostpopularemailprovidershaveputadditional securityframeworksinplacetohelpdetectspoofedemails,including:

- **SenderPolicyFramework(SPF)**:SPFcheckstoseeifthesender's**IPaddress**isassociatedwiththeemaildomain theyareusingwhensendinganemail.
- **DomainKeysIdentifiedMail(DKIM)**:DKIMworkstoverifythattheemailhasn'tbeenalteredbetweenthesender'sand recipient's servers.
- **Domain-basedMessageAuthentication,Reporting,andConformance (DMARC)**:DMARCgivesthesenderthe optiontoinformtherecipientthattheemailisprotectedbySPForDKIM.

Notonlydothesesecuritymeasureshelpalertusersofspamandspoofedemails,buttheycanbeusedtohelpverifyifanemailis legitimate.Tolearnhowyoucanusethesesecurityprotocolstocheckthelegitimacyofamessage,followthefollowingstepsbasedonyour email provider.

HowtocheckSPF,DKIM,andDMARCstatusonGmail:

1. Viewtheemailinquestion.
2. Clickthethree-doticoninthetoprightcorneroftheemail.
3. Select"Showoriginal."

4. Checkandseeiftheemailismarked"pass"or"fail"foreachsection.

HowtocheckSPF,DKIM,andDMARCstatusonOutlook:

1. Viewtheemailinquestion.
2. Clickthethree-doticoninthetoprightcorneroftheemail.
3. Hoverover"View"andthenselect"Viewmessagedetails."
4. Scrollthroughthedetailsandview"Authentication-Results"toseeiftheemailismarked"pass"or"fail"foreachsection.

HowtocheckSPF,DKIM,andDMARCstatusonYahooMail:

1. Viewtheemailinquestion.
2. Clickthethree-doticoninthetoprightcorneroftheemail.
3. Select"Viewrawmessage."
4. Scrollthroughthedetailsandview"Authentication-Results"toseeiftheemailismarked"pass"or"fail"foreachsection.

Bytakingtheseadditionalprecautions,youcanbesurethatyou'redealingwithalegitimatesender,thereforereducingtheriskof aspoofedemailaddressgoingunnoticed.

Howtoprotectagainstemailspoofing:6protectiontips

Email Spoofing Protection Tips

Watch for suspicious email addresses

Avoid clicking links and attachments

Run a search for related scams

Check for grammar and spelling errors

Safeguard your personal information

Use antivirus software

Inadditiontodoingyourbesttoidentifyaspoofedemailbeforeresponding,thereareprecautionsyoucantaketoprotectyourselffromemail spoofing. TohelpkeepyourselfCyber Safewhileusingemail,followtheseprotectiontips:

- **Watchforsuspiciousorunknownemailaddresses**:Oneofthefirstindicatorsofmanyspoofedemailsistheuseofa suspiciousemailaddress.Insomecases,theemailaddresscouldcontaintyposorreplaceletterswithnumbers.

- **Avoid clickinglinksandattachments**: Besuretoavoidclickinganylinksorattachments,asspoofedemailsmay containlinksthatcantakeyouto**maliciouswebsites**orexposeyoutomalware.
- **Runasearchforrelatedscams**:Ifanemailseemssuspicious,copyandpastethecontentsoftheemailintoasearch engine.It’spossiblethattheemailhasbeensenttoothersbefore,anditmayhavebeenreportedasascamsomewhere online.
- **Checkforgrammarandspellingerrors**:Inmanycases,spoofedemailscontainspellingandgrammaticalerrorsthat alegitimatemessagewouldnot.
- **Safeguardyourpersonalinformation**:Alwaysthinktwicebeforesharinganysortofpersonalinformationonline.If youdo,besuretoverifythatyou’resharingitwithareliablepersonororganization.
- **Useantivirussoftware**:**Antivirussoftware**canhelpprotectyourdevicefromthedangersofemailspoofinglike phishing,malware,andidentitytheft.

Nowthatyouhaveabetterunderstandingofemailspoofingandhowyoucanprotectyourselfagainstit,youcanfollowup,circleback, andsendwithconfidence.Aboveall,it’simportanttoalwaysusecommonsenseandbecautious,asthereareotherthreatsthatcanimpactyour **emailsecurity**.

FAQsaboutemailspoofing

Stillhavemorequestions?We’vegotanswers.Readalongtolearnanswerstothesecommonlyaskedquestionsaboutemailspoofing.

What’sthedifferencebetweenaspoofedandhackedaccount?

Thedifferencebetweenaspoofedand**hackedemailaccount**isthatahackedaccountmeansthatthehackerhasgainedfullaccess toyouremailaccount,allowingthemtosendlegitimatemessagesfromyouraddress.Intheeventthatyouremailaddressisspoofed,the **hacker**willonlybeattemptingtomakeitlookasifthemessageiscomingfromyou,buttheywon'thaveaccesstoyouraccount.

Canemailspoofingbetraced?

Generallyspeaking,yes,emailspoofingcanbetraced.ThisisduetoasecurityprotocolknownasSenderPolicyFramework(SPF),which canlocatethesender’sIPaddress.

Cansomeoneusemyemailaddresswithoutmeknowingit?

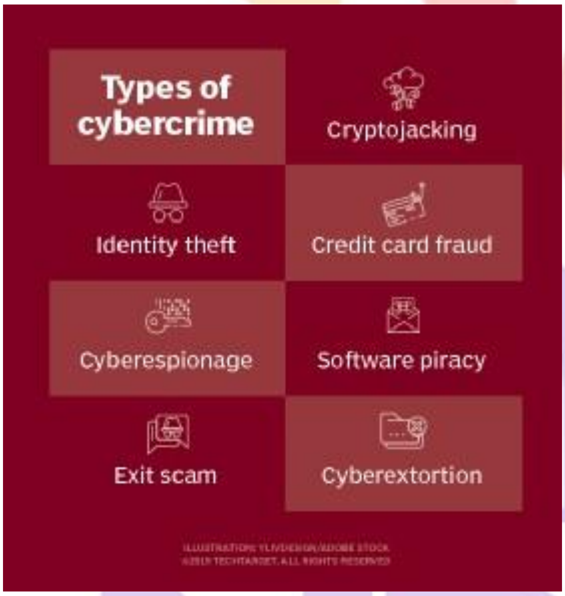
Unfortunately,thereisnowaytocompletelypreventcybercriminalsfromattemptingtouseyouremail address.However,there areprecautionsyoucantaketopreventascammerfromloggingintoyouremailaccount,suchasusingstrongpasswordsand enabling**two-factorauthentication**.

CyberPornography(Exm.MMS):

Cyber-stalking:

Whatiscyberstalking?

Cyberstalkingisacrimeinwhichsomeoneharassesorstalksavictimusingelectronicordigitalmeans,suchassocial media,email,instantmessaging(IM),ormessagespostedtoadiscussiongrouporforum.Cyberstalkerstakeadvantageof the anonymityaffordedbytheinternettostalkorharasstheirvictims,sometimeswithoutbeingcaught,punishedorevendetected.



Theterms*cyberstalking*and*cyberbullying*areoftenusedinterchangeably.Cyberstalking,however,isactuallyaformof cyberbullying,which--alongwithcybersquattingandcyberterrorism--isamongthegrowingnumberofcomputer-andinternet-relatedcrimes,collectivelyreferredtoas*cybercrime*.

Although *cyberstalking* is a generaltermfor onlineharassment, it can take manyforms, including slander, defamation, false accusations,trollingandevenoutrightthreats.Inmanycases,especiallywhenboththeharasserandvictimareindividuals,themotive may be the following:

- monitorthevictim'sonline--and,insomecases,offline--activities;
- trackthevictim'slocationsandfollowthemonlineoroffline;

- annoythevictim;
- intimidate,frighten,controlorblackmailthevictim;
- revealprivateinformationaboutthevictim,apracticeknownas*doxing*;or
- gathermoreinformationaboutthevictimtostealtheiridentityorperpetrateotherreal-worldcrimes,liketheftor harassment.

Cyberstalkers oftenstartsmall. Inthebeginning, they maysend afew strange or somewhatunpleasant messages totheir intendedvictim.Then,later,theymaybrushoffthesemessagesasfunny,annoyingormildlyweirdandignorethemwithouttakingany action.

Overtime,themessagesmaybecomesystematic,sustainedandrepetitiveandtakeonanincreasinglyintimidatingorfrighteningtone.

Direct and indirect cyberstalking

Cyberstalkingcanbedirectorindirect.

Perpetratorsmaydirectly emailtheir victims orfloodtheir inboxes with emails. Ortheymayharassthem throughIM, voicemail, textingorotherformsofelectroniccommunications.Theymayusetechnologiestosurveilorfollowtheirvictimsorcontinuouslyviewtheir pages -- often without their knowledge.

Sometimes,cyberstalkersmaysend obscene, vulgar or offensivecomments,socialmediafollower or friend requests, oreven outrightthreats. Thestalkersmayeitherattackthevictims, whichmaydistressthem,orcausethem tofearfortheirsafety and well-being. They may also attack their victims' family or friends to expand their sphere of stalking influence.

Inindirectcyberstalking attacks,perpetratorsmaydamagethevictim'sdevice.Theymaydothisbyinfectingit withransomwaretolocktheirfilesandthenforcingthem to payaransom forunlockingthem.Ortheymayinstall avirusorkeystrokeloggerthatmonitorsthevictim'sdigitalbehaviorand/orstealsdatafromthedevice.

Aparticulartypeofspywarecalled*stalkerware*canrunonavictim'sinternet-enableddigitaldeviceandcollecttheuser's actionsonthesedevices,includingemails,textmessages,photographsandkeystrokes.

In other indirect attacks, perpetrators may post falseormalicious information about their victims onlinetodamagetheir social standingorprofessionalreputations--aformof*cybersmearing*--orsetupafakesocialmediaorforumaccountintheirvictims'namesto impersonate them and post online material on their behalf.

Cyberstalking:Victimsandcriminals

Often,cyberstalkerspursuetheirvictims overasustainedperiod.Anoverwhelmingmajorityofcyberstalkers aremen,while victims are usually women. However, cyberstalking cases where women were the perpetrators are not unheard of. Forinstance,followingthe2006MeganMeiersuicidecaseinMissouri,afemalecyberstalkerwasindictedandconvictedin2008of violating the Computer Fraud and Abuse Act. Occasionally, men have been victims in some cyberstalking cases.

Victims ofcyberstalkingcouldbeindividuals --matureadults, young adults andchildrenareallsusceptible-- orgroups, organizations orevengovernments.AccordingtotheFederalBureauofInvestigation,childrenandadultsareparticularly vulnerabletooneparticulartypeofcyberstalking:*sextortion*.

Thisiswhenstalkersthreatenavictim withthereleaseofprivateorsensitiveinformationunlessthelattercanmeettheformer's demandsfor sexual favors, nude photos, etc.

Consequencesofcyberstalking

Aspart of acyberstalkingcampaign, astalkermayharass avictim withcontentthat'ssimplyannoyingorinappropriateand more of a nuisancethan anythingelse.Inmoreseriouscases, victims mayhave tocontend withcontentthat'sdisturbing,traumatizing or threatening. They may facesevereforms of online harassment, including sexual harassment and physical threats.

Inalmosteverycyberstalkingcase,victimsfeelannoyedatbestandfearfulatworst.Confusion,angerandanxietyarecommon among victims.Somemayalsoexperienceinsomniaorsuffer fromphysicalailments,likeheadaches,acidrefluxor stomachulcers,or mental ailments, like depression or post-traumatic stress disorder. In extreme cases, they may become suicidal.

Iscyberstalkingacrime?

Cyberstalkingisacrimeismanycountries,includingtheUnitedStates.However,legislationtopreventcyberstalkingandtopunish apprehended cyberstalkers varies from country to country and, in the case of the U.S., even from state to state.

CaliforniawasthefirstU.S.statetopassacyberstalkinglawin1999.OtherU.S.stateswithatleastsomekindofcyberstalkinglegislation include the following:

- Alabama
- NewYork
- Illinois
- Hawaii
- Arizona
- Texas

- Florida

Missouri's anti-cyberstalkinglaw,meanttocriminalizetheuseoftheinternettoharasssomeone,waswrittenafterthe aforementioned Megan Meier case.

Since2000,U.S.federallawspecificallyaddressescyberstalkingundertheViolenceAgainstWomenAct.Thepunishmentfor cyberstalking ranges from monetary fines to time in prison.

Othercountriesthathaveanti-cyberstalkinglegislationinplaceincludethefollowing:

- Australia
- Canada
- Philippines
- India
- Pakistan
- Nigeria
- Singapore
- SouthAfrica

IntheU.K.,cyberharassmentisaprosecutablecrimeundertheProtectionfrom HarassmentAct1997ortheMalicious Communications Act 1988. Some countries like Singapore also have laws to prosecute internet trolls.

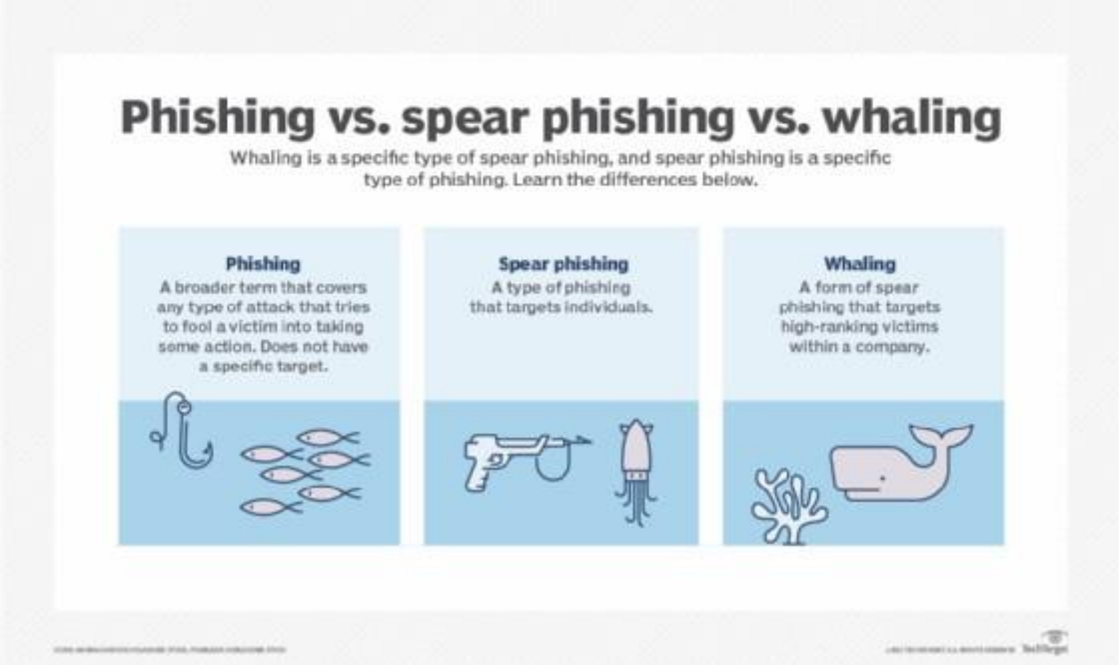
Thepracticeofdoxing,theonlinepublicationofauser'spersonalandidentifyingdata,isconsideredaviolationofArticle8ofthe European Convention on Human Rights.

Howtoguardagainstcyberstalking

Individuals can guard againstcyberstalking withoutlosingtheir onlineindependence.Onestrategyistostayas anonymous as possible. Ofcourse,completeanonymityis almost impossibleontheinternetnowadays, sothenext bestthingistokeepalow profile, especially on social media.

Ratherthanhavinganidentifiableandtraceableonlinepresence,usenicknames and/orgender-neutralnames whenpossible.Avoid postingpersonaldetails,suchas your emailaddress,homeaddress,phonenumber orworkplacedetails,online,whereanyone can easily access them and use them to cyberstalk. Also, guard photographs, and make sure all private information, like vacation plans, photos and posts, are visible only to trusted individuals.

Useaprimaryemailaccountonlyforcommunicatingwithknown/trustedpeople,andsetupananonymous emailaccountforall other communications. Install email spam filters to minimize spam and the possibility of email-based phishingor cyberstalking attacks.



Phishing vs. spear phishing vs. whaling

Whaling is a specific type of spear phishing, and spear phishing is a specific type of phishing. Learn the differences below.

Phishing
A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

Spear phishing
A type of phishing that targets individuals.

Whaling
A form of spear phishing that targets high-ranking victims within a company.

Otherwaystoguardagainstcyberstalkingincludethefollowing:

- updateallsoftwaretopreventinformationleaks;
- maskyourInternetProtocoladdresswithavirtualprivatenetwork;
- strengthenprivacysettingsonsocialmedia;
- strengthenalldeviceswithstrongpasswordsor,better,usemultifactorauthentication;
- avoidusingpublicWi-Finetworks;
- sendprivateinformationviaprivatemessages,notbypostingonpublicforums;
- safeguardmobiledevicesbyusingpasswordprotectionandneverleavedevicesunattended;
- disablegeolocationsettingsondevices;
- installantivirussoftwareondevicestodetectmalicioussoftware;
- alwayslogoutofallaccountsattheendofasession;and
- bewareofinstallingappsthatasktoaccessyourpersonalinformation.

Multifactor authentication
Time
Location
Something you have
Something you are
Something you know
55984
*****

ART: MYKYTA/ADOBE STOCK, ALEXDNDZ/ADOBE STOCK
©2022 TECHTARGET. ALL RIGHTS RESERVED.

Multifactorauthenticationrequires,asthenameindicates,usingmultiplefactorstoauthenticateidentity.Thesecouldinclude somethingyou know(say, apassword),something youhave(say, asmartphone)orsomethingyou are(say,biometrics--fingerprints, face ID, etc.).

Whattodoif cyberstalked

Shouldanindividualbecomethevictimofacyberstalker,it'simportanttotakeimmediateaction.

Themosteffectivecourseofactionistoreporttheoffendertotheirinternetserviceprovider(ISP).Shouldthatoptionbe ineffective,theyshouldchangetheirISPandallonlinenames.

Blocktheperson,evenifthesemessagesarenotyetthreatening.Also,reportthemtotheplatform,especiallyifthey'reharassing, stalking or threatening. Most social media platforms make it easy to report abusive behavior. These includeFacebook,TwitterandLinkedIn.

Ifthestalkinghasbecomethreateningorfrightening,saveevidence,andcontactlawenforcement.Also,minimizetheamount ofinformationthat'savailableonlineand/orincreasetheamountoffakedecoyinformationaboutyoutomisleadcyberstalkers.