CONTENTS

3:Online banking

4: National Cyber Security Policy -2013

5: INFORMATION SECURITY BEST PRACTICES

From the Editor's Desk

It is, of course, no exaggeration to endorse the fact that Information Technology has taken our world by storm. Its tentacles are far-fetched and all pervading. We have become so dependant and inseparable that we cannot, possibly, imagine a day without its presence. Be it in business, education, medicine, policing, government functions, agriculture, space and whatnot, its awesome need and presence is felt everywhere. In fact, we are so hooked and addicted to technology in this amazing era of unprecedented connectivity, convergence and integration of all sorts of technology. Right from the simplest machines like calculators to the most complicated ones like space craft, IT can be seen at play. However, the agility and convenience it offers is not without its flipside. With high proliferation of internet enabled devices and increased access to the world wide web, internet related crimes and criminals have been on the rise.

We, the Kerala Police, have always been in the forefront to harness new trends in all fields and IT is no exception. All efforts are being made to tap these potentials into improving our service delivery mechanisms so that the recipient public fully benefits from these new advances. At the same time we have to ensure that they are guarded and protected from its negative impacts. Training is the key with which we can unlock our minds into these new domains like machine learning, artificial intelligence, block chain technology, Internet of things (IoT) etc. With this view, the year 2019 has been declared as the year of Cyber Training for Kerala Police. Basic as well as advanced and specialized cyber-related courses are organized in our training institutions to provide greater insight into these new technologies. This will help to keep our workforce to keep abreast with new technologies and to move well ahead in utilizing these innovations. We also need to

be a lot smarter and faster to prevent and detect the new age crimes associated with this technology.

Janamaithri Police work in tandem with the public and are concerned with all matters affecting public life. This journal of Janamaithri Police attempts to provide a glimpse on just a few general aspects of the Cyber Technology. The articles presented in the journal are compiled and written by officer of Kerala Police who have taken part in the "Advanced course of cyber security" organised at the police Training College Thiruvananthapuram from 12-09-2018 to 25-10-2018.Though it is only a tip of the iceberg, due to the voluminous nature of the topic the present volume is published in two parts. Part 1 deals with topics like 'Intellectual Property Rights in Cyber Space', Internet of things (IoT), Online Banking etc. In addition, the MHA guidelines on the subject 'Information Security: Best Practices' is annexed in Part 1. It is followed by part 2 which includes detailed study reports on a few commonly committed cyber crimes like Spoofing, OTP frauds and Cyber Stalking. It also incorporates the 'Framework & Guidelines for use of Social Media for Government Organizations' published by the Department of Electronics and Information Technology. It is sincerely hoped that this journal would provide very exhaustive information, though not extensive, on certain contemporary and relevant areas of concern in today's cyber world.

Dr.B.Sandhya IPS

INTELLECTUAL PROPERTY RIGHTS IN CYBER SPACE

Abstract

This paper is an attempt to portray IPR in the realms of Cyber Space. In India, the existing intellectual property regime that deals with the protection of computer software is the Indian Copyright Act, 1957. At present, legal system and framework are inadequate to address all the aspects of Information Technology (IT). Grey areas do exist in the legal system. Convergence Law in India aims to promote, facilitate and develop in an orderly manner the carriage and content of communications including broadcasting, telecommunications and multimedia.

Information Technology Act 2000 does not mention a single word about Intellectual Property protection while infringement of IPR is one of the most challenging areas in cyberspace. With regard to copyright and Domain names, violations do occur on the internet but Copy Right Act 1957 & Trade Mark Act 1999 are silent on that. Therefore we have no enforcement machinery to ensure the protection of domain names on net. Time has come where we must enact special legislation for the protection of Intellectual property in cyberspace.

Introduction

Property is a thing or right that can be owned or that have a money value. Corporeal property and Incorporeal property are the two classifications of property. An intangible, incorporeal proprietary right over immaterial things such as patent right, copy right, right to trade mark, right to design etc. are called Intellectual Property Rights (IPR). These are the rights granted to the creators of IP, and include trademarks, copyright, patents, industrial design rights, and in some jurisdictions trade secrets. Artistic works including music and literature, as well as discoveries, inventions, words, phrases, symbols, and designs can all be protected as intellectual property. Likewise Cyber Space is a term which is being derived from a Science-Fiction movie by Mr. Fred Roderick in the year 1920, and the term actually describes the virtual world which is something apart from the real world.

Property – things and rights that can be owned or that have a money value.

Proprietary right is a *right in rem* Rights in rem are almost always negative. It is a right to be left alone. It is a right that people should not interfere with the ownership.

PROPERTY

1. Corporeal property.
2. Incorporeal property.

CORPOREAL PROPERTY

1. Movable property.
2. Immovable property.

INCORPOREAL PROPERTY

1. Proprietary right over immaterial things eg. goodwill, patent right, copy right, right to trade mark, right to design etc.
2. Right in *re aliena* (right of a person over the material thing owned by another person) – eg. Easement right, right of lessee, right of mortgagee, right of pledgee etc.

Intellectual property Rights

Intellectual property Rights is a category of property rights that includes intangible creations of the human intellect, and primarily encompasses copyrights, patents, and trademarks. It also includes other types of rights, such as trade secrets, publicity rights, moral rights, and rights against unfair competition.

Categories of Intellectual Property

- Patents
- Trademarks
- Design
- Copyright
- Trade Secrets
- Geographical Indications
- Integrated Circuits
- Plant Breeders Rights

Applicability of Intellectual Property rights in Cyber World

What is copyright in cyberspace means?

Copyright on the web seems to be a difficult concept for some people to understand. But it's really simple: If you did not write or create the article, graphic, or data that you found, then you need permission from the owner before you can copy it. Remember, when you use someone's graphic, HTML, or text without permission, you are stealing, and they can take action against you.

Relation between Internet and Copyright

So far international copyright law was based upon the Berne Convention for the protection of literary and artistic works and the T.R.I.P.S (Trade Related aspects of Intellectual Property Right) of 1995. Since 1974, the international copyright instruments have been managed by a special United Nations Agency by name W.I.P.O (World Intellectual Property Organisation). W.I.P.O's objective as per the

treaty is to promote the protection of intellectual property throughout the World through cooperation among the states and where appropriate, in collaboration with other international organizations. Currently W.I.P.O consists of 180 member states. W.I.P.O administers six copyright treaties and aims at "homogenizing national intellectual property protections with an ultimate eye towards the creation of a unified, cohesive body worldwide international law."

The T.R.I.P.S (Trade Related Aspects of Intellectual Property Rights) Agreement, The General Agreement on Tariffs and Trade (G.A.T.T) has also addressed copyright issues, in parallel to W.I.P.O. The goal of G.A.T.T is to promote the reduction of tariff barriers to the international movement of goods. In 1994, the Uruguay round of G.A.T.T produced T.R.I.P.S. The same round also instituted the W.T.O (World Trade Organisation). The T.R.I.P.S Agreement adopts portions of the Berne, Rome and Paris Conventions in enunciating norms for intellectual property laws.

W.I.P.O (World Intellectual Property Organisation)

W.I.P.O is an organization of the United Nations (U.N). W.I.P.O's activities are of four kinds:- Registration, promotion of inter-governmental cooperation in the administration of intellectual property rights, specialized programme activities and lastly dispute resolution facilities. In 1996, member countries found it necessary to form a treaty to deal with the protection of copyright evolvement of new technology.

Intellectual Property Right disputes

Cyber Squatting, Domain Name Disputes, Inline Linking, Copy right violation in Website are some Intellectual Property Right disputes on the cyber space.

Cyber Squatting

Cybersquatting is a type of Cyber crime which is illegal domain name registration or use. It is an act of obtaining fraudulent registration with an intent to sell the domain name to the lawful owner

of the name, at a premium. An individual or a company registers a domain name and such domain name is identical or similar to a trademark of any other party and maliciously tries to sell the same for a profit this is known as “Cybersquatting”. Cyber squatting is also known as domain squatting.

Example: A cyber squatter could buy *Heinz.com* if the company hadn't created a website yet, looking to sell the domain to Heinz at a later date for profit, or use the domain name to attract traffic and generate money through advertising

Legal Aspects

Unlike many developed countries, in India we have no Domain Name Protection Law and Cyber squatting cases are decided under Trademark Act 1999.

That although the Indian Courts have drawn the distinction between trade mark and domain name; wherein the Hon’ble Supreme Court in Satyam Infoway Ltd VsSifynet Solutions Pvt Ltd; AIR 2004SC3540 has observed that the

"*distinction lies in the manner in which the two operate. A trademark is protected by the laws of a country where such trademark may be registered. Consequently, a trade mark may have multiple registrations in many countries throughout the world. On the other hand, since the internet allows for access without any geographical limitation, a domain name is potentially accessible irrespective of the geographical location of the consumers. The outcome of this potential for universal connectivity is not only that a domain name would require worldwide exclusivity but also that national laws might be inadequate to effectively protect a domain name*".

Domain Name Disputes

It is a conflict that arises when more than one individual or group believes that it has the right to register a specific domain name. The disputes generally arise over second level domain names as no two identical second level domain names can exist under a same top

level domain name. The second level domain name is the name directly to the left of the top level domain name in an internet address.

Eg. In www.facebook.com, the second level domain name is facebook

What is Domain Name

A domain name is the address where Internet users can access your website. A domain name is used for finding and identifying computers on the Internet. Computers use IP addresses, which are a series of number. However, it is difficult for humans to remember strings of numbers. Because of this, domain names were developed and used to identify entities on the Internet rather than using IP addresses.

Classification of Domain Names

(1) Top Level Domain (TLD)
(2) Second Level Domain(SLD)
(3) Sub Domain (SD)

Eg. Blog.FusionLawSchool.com

Top Level Domain - .com,
Second Level Domain –Fusion Law School
Sub Domain – blog

Top Level Domain Names are classified into 2

(1) General Top Level Domains (gTLDs)
(2) Country Code Top Level Domains (ccTLDs)

General Top Level Domain

1. .com – (Commercial Enterprises)
2. .org – (Non Profit Organizations)
3. .net – (Network/Internet related Organizations)
4. .edu – (College/Universities)
5. .gov – Government Entities)

Country Code Top Level Domain

- .ca – for Canada
- .in – for India

The domain name dispute tend to fall in to 4 categories

1. Cyber Squatters.
2. Cyber Parasites.
3. Cyber Twins.
4. Reverse Domain Name Hi-Jacking.

Cyber Squatters –

Who have speculatively registered or have acquired the domain name for the purpose of selling, lending or otherwise transferring the domain name registration to the owner of trademark or serviceman or even to a competitor.

British Telecommunication Vs. One in a Million (The Court of Appeal ruled in favour of plaintiff)

Cyber Parasites

They also expect to gain financially. Unlike cyber squatters such gain is linked to the use of domain name. They register a domain name that is similar to or is commonly mistyped version of a famous organization.

Eg.Rediff Communication Limited Vs. Cyberbooth (radiff.com) (The Court of Appeal ruled in favour of plaintiff since both parties had a common field of activity)

Cyber Twins

When both parties have a legitimate claim to a domain name then they are known as Cyber Twins

Eg. Indian Farmers Fertiliser Corporation Ltd. Vs. International Foodstuffs Co.

The dispute was relating to the domain name - *www.iffco.com*

The complainant had alleged the defendant of diverting the internet users to its own website. The Arbitration Centre dismissed the case as both the parties had legitimate interest in the domain name and the complainant had failed to prove 'bad faith' on the part of the defendant.

Reverse Domain Name Hijacking

It occurs where a rightful trademark owner attempts to secure a domain name by making cyber squatting claims against a domain name's cyber squatter owner. It is an attempt by a trade mark holder in bad faith to take control of a domain name from another who is not in breach of trade mark laws and who has a legitimate interest in the name.

Reverse domain name "hijacking" is a legal remedy to counter the practice of domain squatting, wherein individuals hold many registered domain names containing famous third party trademarks with the intent of profiting by selling the domain names back to trademark owners. Trademark owners initially responded by filing cybersquatting lawsuits against registrants to enforce their trademark rights. However, as the number of cybersquatting incidents grew, trademark owners noticed that registrants would often settle their cases rather than litigate. Cybersquatting lawsuits are a defensive strategy to combat cybersquatting, however such lawsuits may also be used as a way of strongarming innocent domain name registrants into giving up domain names that the trademark owner is not, in fact, entitled to.

In-lining or 'In-line linking

Many websites have Audio or image or picture or video files on their website. It is possible for any person to link these in their own website in such a way that they appear as a part of the website to which it is linked. This is called inline link or hot link. In case any copyright or trade marks in the file, then their appearance on the other website, without permission of the owner is illegal.

When a web site is visited, the browser first downloads the textual content in the form of an HTML document. The downloaded HTML document may call for other HTML files, images, scripts and/or stylesheet files to be processed. These files may contain <img> tags which supply the URLs which allow images to display on the page. The HTML code generally does not specify a server, meaning that the web browser should use the same server as the parent code (<imgsrc="picture.jpg" />). It also permits absolute URLs that refer to images hosted on other servers (<imgsrc="http://www.example.com/picture.jpg" />).

When a browser downloads an HTML page containing such an image, the browser will contact the remote server to request the image content.

Common uses of linked content

The ability to display content from one site within another is part of the original design of the Web's hypertext medium. Common uses include:

- It is copyright infringement to make copies of a work for which you have no license, but there is no infringement when you provide a simple text link within an HTML document that points to the location of the original image or file (simply called a "link").
- Web architects may deliberately segregate the images of a site on one server or a group of servers. Hosting images on separate servers allows the site to divide the bandwidth requirements between servers. As an example, the high-volume site Slashdot stores its "front page" at slashdot.org; individual stories on servers such as games.slashdot.org or it.slashdot.org; and serves images for each host from images.slashdot.org.
- An article on one site may choose to refer to copyrighted images or content on another site via inline linking, which may

avoid rights and ownership issues that copying the original files could raise. However, this practice is generally discouraged due to resulting bandwidth loading of the source, and the source provider is often offended because the viewer is not seeing the whole original page, which provides the intended context of the image.

- Many web pages include banner ads. Banner ads are images hosted by a company that acts as middleman between the advertisers and the web sites on which the ads appear. The <img> tag may specify a URL to a CGI script on the ad server, including a string uniquely identifying the site producing the traffic, and possibly other information about the person viewing the ad, previously collected and associated with a cookie. The CGI script determines which image to send in response to the request.
- Some websites hotlink from a faster server to increase client loading speed.
- Hit counters or Web counters show how many times a page has been loaded. Several companies provide hit counters that are maintained off site and displayed with an inline link.

Controversial uses of inline linking

The blurring of boundaries between sites can lead to other problems when the site violates users' expectations. Other times, inline linking can be done for malicious purposes.

- Content sites where the object is stored and from which it is retrieved may not like the new placement.
- Inline linking to an image stored on another site increases the bandwidth use of that site even though the site is not being viewed as intended. The complaint may be the loss of ad revenue or changing the perceived meaning through an unapproved context.

- Cross-site scripting and phishing attacks may include inline links to a legitimate site to gain the confidence of a victim.
- Pay-per-content services may attempt to restrict access to their content through complex scripting and inline linking techniques.
- Inline objects can be used to perform drive-by attacks on the client, exploiting faults in the code that interprets the objects. When an object is stored on an external server, the referring site has no control over if and when an originally beneficial object's content is replaced by malicious content.
- The requests for inline objects usually contain the referrer information. This leaks information about the browsed pages to the servers hosting the objects (see web visitor tracking).

Prevention

Client side

Most web browsers will blindly follow the URL for inline links, even though it is a frequent security complaint. Embedded images may be used as a web bug to track users or to relay information to a third party. Many ad filtering browser tools will restrict this behaviour to varying degrees.

Server side

Some servers are programmed to use the HTTP referrer header to detect hotlinking and return a condemnatory message, commonly in the same format, in place of the expected image or media clip. Most servers can be configured to partially protect hosted media from inline linking, usually by not serving the media or by serving a different file.

URL rewriting is often used (e.g., mod_rewrite with Apache HTTP Server) to reject or redirect attempted hotlinks to images and media to an alternative resource. Most types of electronic media can

be redirected this way, including video files, music files, and animations (such as Flash).

Other solutions usually combine URL rewriting with some custom complex server side scripting to allow hotlinking for a short time, or in more complex setups to allow the hotlinking but return an alternative image with reduced quality and size and thus reduce the bandwidth load when requested from a remote server. All hotlink prevention measures risk deteriorating the user experience on third party website.

In-lining or 'In-line linking' enables a web page to summon different elements from diverse pages or serves to create a new web page.

Instead of copying the elements to the composite page, the elements are linked in by "pulling in" graphic or image files from another site and displaying on the composite web page.

In India, Section 52 of the copyright act explains which acts are not infringements of copyright.

Copy right violation in Website

There are many websites that permit uploading of video and audio files. However people are not only uploading their own video and audio files but are also uploading the film clips and music files that are copyright of others.

Even if video or audio CD is legally purchased, is does not mean that it can be played as one likes. Its use is determined by the terms and conditions of the sale The CDs normally contain a notice of the following kind:

'All rights reserved. For private use only. Unauthorised copying, public performance, broad casting, screening, playing is prohibited.

This means that sale is merely a license to listen or watch the CD privately; it cannot be played publicly.

The websites always prohibit uploading or copyrighted material. The website has to delete the material on notice otherwise they will also be liable for copyright violations or copyright infringement.

Spotting Copyright Infringement

The first thing you should do is visit http://www.copyscape.com/, enter the website URL for your home page and run a search.

If results come back, text may already have been stolen from your website. If no results are returned, there still may be issues with content from other pages of your website. You can check other URLs with the tool above. Focus on high-traffic and/or SEO page targets.

To get automatic alerts of possible copyright infringement, invest in a weekly subscription to Copysentry. With this tool, you can enter a list of all URLs that you want tracked. Then, each week you will get an email containing websites that have text that matches the website URLs you are tracking.

Tracking Copyright Infringement Cases

The easiest way to track copyright infringement cases is to keep a spreadsheet with the columns noted below.

When you get your weekly email from Copy sentry, these are the steps you will follow:

1. Click the link in the email to visit the website and determine if the website has stolen your copy.
2. Populate the spreadsheet fields as follows:
    a. Date Sent
        - Enter today's date.
    b. Date Resolved
        - Leave blank for now.

c. Resolution
   - Leave blank for now.

d. Domain
   - Enter the offending domain in the format of domain.com.

e. IP Address
   - Open a command prompt and ping the domain (ex. ping domain.com) of the offending website.
   - Enter the IP address that is returned.

f. Hosting Company

   Visit https://www.arin.net.
   - In the top right corner, enter the IP address and click the search button.
   - Enter the hosting company that is returned.

g. Contact

   - From the same step above, look for an email address that starts with "abuse@".

      I. Enter this email as your contact for now.

      II. Do a Google search for "hosting company dmca" replacing this with the actual hosting company name.

      III. See if you can find a page on the hosting company's website that describes its DMCA (Digital Millennium Copyright Act) process.

      IV. You should be able to find a DMCA form or page that provides the DMCA email contact it would like you to use.

      V. If you find a DMCA form or specific DMCA email address, update your spreadsheet to track this info instead of the abuse@ email address.

h. Copyscape URL

- Enter the Copyscape URL.

Repeat this process each week as you get a new email from Copysentry.

Resolving Copyright Infringement Cases

Once you are uncovering and tracking instances of copyright infringement, you will want to start the process to resolve these cases. There are four main scenarios that you will be dealing with:

1. Hosting Company Provides a DMCA Form

If the hosting company provides a DMCA form (example from hostgator.com), then you can easily fill out the form and submit your DMCA take down request.

2. Hosting Company Doesn't Provide a DMCA Form

Most of the time, the hosting company will not have a DMCA form. In these cases, you will need to draft a formal DMCA take down notice and send it via email to the hosting company.

The first thing you will need is a template DMCA letter. This site provides a sample DMCA take down notice. You should create a template Word document containing the letter and then populate it each time you have a copyright infringement case. In the letter, I recommend including the offending IP address and Copyscape URL. Also, I recommend adding a screenshot of the Copyscape URL/page that highlights the stolen copy, and creating a PDF of the final document. Make sure to save copies of these documents for future reference.

Next, create a new email and attach the PDF. You will be sending it to the hosting company's abuse@ email (or a more specific DMCA email). The subject of the email can be DMCA Take Down Notice for [domain.com]. The body of the email can simply state:

Please find a DMCA take down notice attached regarding [domain.com] hosted at [IP Address]. If you need further information, please let me know. Otherwise, I await your response.

Once you send this notice to the hosting company, you should hear back within a few days. The hosting company should then send your notice to its client and ask the client to remove the infringing content. Once the client removes the content, the hosting company will close the case and alert you. If the client does not remove the infringing content, the hosting company will disable the specific page or entire website.

3. Hosting Company Is Outside the USA

If the hosting company is outside the USA, chances are it will not honor DMCA take down requests. However, many international hosting companies do have terms posted on their websites regarding copyright infringement. You should send an email to the hosting company using the abuse@ email address. In that email, tell the hosting company who you are, the website you own, the web page URL that has your original text, along with the offending website URL and IP address. You can also include the Copyscape URL and a screenshot of the offending page. State that this is a case of copyright infringement and that you are requesting the hosting company to take down the offending page. Many international providers will work with their client to remove the infringing copy or take down the page.

4. Hosting Company Seems to be Cloud Flare (or another cloud-based website security application)

If the offending IP address lookup at https://www.arin.net comes back with Cloud Flare as the hosting company, you will need to complete its DMCA form to file your notice. Cloud Flare is a cloud-based website security application and not an actual hosting company. One of the aspects of its service is to hide the hosting company information. By completing its DMCA form, Cloud Flare will send your request to its client and the hosting company. Many times, you will need to draft a formal DMCA notice directly to this hosting company.

Other cloud-based website security companies have similar methods to handle DMCA requests.

Once you receive communication from the hosting company, you can update your copyright tracking spreadsheet. As you resolve copyright issues, you should have a cycle where you go back and check old cases to make sure websites did not revert to the infringing content. You can do this by reviewing the Copyscape URLs from past cases.

Investigation

Association of Chief Police Officers (ACPO)

This forensic investigation will be conducted as per Association of Chief Police Officers (ACPO) guidelines and its four principles as well. There are four ACPO principles involved in computer-based electronic evidence. These principles must be followed when a person conducts the Computer Forensic Investigation. The summary of those principles are as follows (ACPO, 2013);

Principle 1: Data stored in a computer or storage media must not be altered or changed, as those data may be later presented in the court.

Principle 2: A person must be competent enough in handling the original data held on a computer or storage media if it is necessary, and he/she also shall be able to give the evidence explaining the relevance and course of their actions.

Principle 3: An audit trail or other documentation of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: A person who is responsible for the investigation must have overall responsibility for accounting that the law and the ACPO principles are adhered to.

Collection

"The collection phase is the first phase of this process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data" (CJCSM 6510.01B, 2012). There are two different types of data that can be collected in a computer forensics investigation. They are volatile data and non-volatile data (persistent data). Volatile data is data that exists when the system is on and erased when powered off, e.g. Random Access Memory (RAM), registry and caches. Non-volatile data is data that exists on a system when the power is on or off, e.g. documents in HD. Since volatile data is short-lived, a computer forensic investigator must know the best way to capture it. Evidence can be collected locally or remotely.

The following are the steps to be taken while investigating Intellectual Property Right Dispute:

1) Registration of FIR.
2) Gathering all available information from the assessing the incident.
3) Obtaining information of the networks, network devices such as router, switches, hub, etc.
4) Identifying the external storage devices such as pen drive, flash drive, external hard disk, CD, DVD, memory cards and remote computer.
5) Identifying the forensic tools which can be used in this investigation.
6) Capturing live network traffic in case the suspicious activities are still running
7) Documenting all the activities during the investigation which may be used in court to verify the course of action that was followed in the investigation.
8) Imaging the target devices' hard drive and hashing them with MD5 for data integrity.
9) Analysing the image by competent authority and fix the culprit.

Competent Court

In India, a suit may be instituted in any Court of original jurisdiction, subject to their pecuniary and territorial jurisdiction. In relation to IPR litigation, the designation of the lowest court is "District and Sessions Judge". These cases can also be filed in the High Court, directly, if such High Court is having original jurisdiction. The jurisdiction of the High Court can be invoked, subject to the payment of court fees. The structure of court fees payable varies from State to State.

Border Control Measures for Enforcement of IPR

The Government of India under Section 11 of the (Indian) Customs Act, 1962, is empowered to prohibit importation and exportation of goods of specified description, if it deems necessary to do so. The provision, inter alia, empowers the government to prohibit the import or export of goods for 'the protection of patents, trademarks and copyrights. The goods imported in contravention of the provisions of the Customs Act or any other laws for the time being in force are liable to be confiscated. In this regard, a customs officer is empowered to inspect any premises, conveyance, x-ray any person and effect search and seize in case where they have reasons to believe that the goods are of contraband nature. They can also investigate or interrogate any person and arrest him.

Intellectual Property Rights (Imported Goods) Enforcement Rules, 2007

India has notified the Intellectual Property Rights (Imported Goods) Enforcement Rules, 2007. The rules comply with border measures as required by the TRIPS Agreement empowering the Customs Officers to enforce IPR over the imported products. Actions under Customs Act are independent to the remedies provided under various statues on Intellectual Property. As per Rule 2(b) of the Intellectual Property Rights (Imported Goods) Enforcement Rules, 2007, Intellectual Property includes patents, designs, and geographical indications together with trademarks and copyrights.

Upon receipt of the application, in the prescribed format, the Custom Authorities may register the Complaint and enforce Border Control measure for the protection of the Intellectual Property Rights. It is important to note that this right is not unfettered. Certain provisions have been also made and an elaborate procedure has been laid down for the release of the seized goods upon an application of the importer of the goods.

INTERNET OF THINGS

TEAM MEMBERS

1. Dileesh, Sub Inspector of Police, KunnathunadaPS, Ernakulam Rural
2. Arunchand C , CPO 7094, Kidangoor PS, Kottayam
3. Sushin S S, CPO 11474, Cyberdome, Thiruvananthapuram City
4. Sherlin Raj, CPO 6571, DCRB, Thiruvananthapuram City
5. Nikheesh, CPO 6159, DHQ, Malappuram
6. Hareesh K, CPO 2903, Cyber Cell, Kasaragod
7. Kiran Chand, PC 12987, SAP, Thiruvananthapuram
8. Vishnu M T, PC 13012, SAP, Thiruvananthapuram
9. Sajidas Krishnan, PC 9369, KAP 1 Bn, Thrissur
10. Athul Raj, PC 7957, KAP 3 Bn, Adoor, Pathanamthitta

Acknowledgement

This project report on Internet of Things is submitted as a part of Advanced Course on Cyber Crime Investigation conducted at PTC Thiruvananthapuram from 12-09-2018 to 25-10-2018. The course members were divided into various groups and ours was the 1st group formed under the leadership of Sri.Dileesh, Sub Inspector of Police, Kunnathunada, Ernakulam Rural.

We are submitting this project report in a brief span of time with the help of PTC authorities and also utilizing the vast possibilities in the web world. We are expressing our sincere gratitude to The Principal, The Vice Principal, Course coordinator, Indoor and Outdoor staffs of PTC, facilities offered by CDAC, FSL and facilities from various establishment for making us familiar with the cybercrime investigation and also giving us valuable direction for completing the project.

INTRODUCTION

What is IoT ?

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data.

IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. With the arrival of driverless vehicles, a branch of IoT, i.e. the Internet of Vehicle starts to gain more attention.

HISTORY

The definition of the Internet of things has evolved due to convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things.

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994, Reza Raji described the concept in IEEE Spectrum as small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned Device to

Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.

The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he prefers the phrase "Internet *for* things". At that point, he viewed Radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.

A research article mentioning the Internet of things was submitted to the conference for Nordic Researchers in Logistics, Norway, in June 2002, which was preceded by an article published in Finnish in January 2002. The implementation described there was developed by Kary Främling and his team at Helsinki University of Technology and more closely matches the modern one, i.e. an information system infrastructure for implementing smart, connected objects.

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.

APPLICATION

The extensive set of applications for IoT devices is often divided into consumer, commercial, industrial, and infrastructure spaces.

Consumer applications

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.

Smart home

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. Long term benefits could include energy savings by automatically ensuring lights and electronics are turned off.

A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's HomeKit, manufacturers can get their home products and accessories be controlled by an application in iOS devices such as the iPhone and the Apple Watch. This could be a dedicated app or iOS native applications such as Siri. This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo, Apple's HomePod, and Samsung's Smart Things Hub.

Elder care

One key application of smart home is to provide assistance for those with disabilities and elderly individuals. These home systems use assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing impaired users. They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life.

The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that EIoT will account for 9.1 billion devices.

Commercial applications

Medical and healthcare

The **Internet of Medical Things** (also called the **internet of health things**) is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. This 'Smart Healthcare', as it can also be called, led to the creation of a digitized healthcare system, connecting available medical resources and healthcare services.

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost." Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used "to analyze, capture, transmit and store health statistics from multiple resources, including sensors and other biomedical acquisition systems".

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. These sensors create a network of intelligent sensors that are able to collect, process, transfer and analyse valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility

with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

As of 2018, IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients and others involved (i.e. guardians of patients, nurses, families, etc.) to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to the patient's information. Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices and mobile apps to track customer behaviour. This can lead to more accurate underwriting and new pricing models.

Transportation

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance. In Logistics and Fleet Management for example, The IoT platform can continuously monitor the location and conditions of cargo and assets via wireless sensors and send specific alerts when management exceptions occur (delays, damages, thefts, etc.). If combined with Machine Learning then it also helps in reducing traffic accidents by introducing drowsiness alerts to drivers and providing self driven cars too.

Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature:

- The integration of the Internet with building energy management systems in order to create energy efficient and IOT driven "smart buildings".
- The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviors.
- The integration of smart devices in the built environment and how they might to know who to be used in future applications.

Industrial applications

Manufacturing

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyber physical space, it opens the door to create whole new business and market opportunities for manufacturing. Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together.

Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to

asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.

The term industrial Internet of things (IIoT) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT. IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0. It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT may generate $12 trillion of global GDP by 2030.

Design architecture of cyber-physical systems-enabled manufacturing system

While connectivity and data acquisition are imperative for IIoT, they should not be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over the total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the *5C* (connection, conversion, cyber, cognition, configuration) architecture, and it will

transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes.

An IoT-enabled intelligent system of such cases was proposed in 2001 and later demonstrated in 2014 by the National Science Foundation Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at the University of Cincinnati on a bandsaw machine in IMTS 2014 in Chicago. Bandsaw machines are not necessarily expensive, but the bandsaw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, advising users when is the best time to replace the belt. This will significantly improve user experience and operator safety and ultimately save on costs.

Agriculture

There are numerous IoT applications in farming such as collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. This data can be used to automate farming techniques, take informed decisions to improve quality and quantity, minimize risk and waste, and reduce effort required to manage crops. For example, farmers can now monitor soil temperature and moisture from afar, and even apply IoT-acquired data to precision fertilization programs.

In August 2018, Toyota Tsusho began a partnership with Microsoft to create fish farming tools using the Microsoft Azure application suite for IoT technologies related to water management. Developed in part by researchers from Kindai University, the water pump mechanisms use artificial intelligence to count the number of fish on a conveyor belt, analyze the number of fish, and deduce the effectiveness of water flow from the data the fish provide.

The specific computer programs used in the process fall under the Azure Machine Learning and the Azure IoT Hub platforms.

Infrastructure applications

Monitoring and controlling operations of sustainable urban and rural infrastructures like bridges, railway tracks and on- and offshore wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. IoT can benefit the construction industry by cost saving, time reduction, better quality workday, paperless workflow and increase in productivity. It can help in taking faster decisions and save money with Real-Time Data Analytics. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

Metropolitan scale deployments

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is gradually being built, with approximately 70 percent of the business district completed as of June 2018. Much of the city is planned to be wired and automated, with little or no human intervention.

Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants has already seen 18,000 downloads of its city smartphone app. The app is connected to 10,000

sensors that enable services like parking search, environmental monitoring, digital city agenda, and more. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification.

Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. French company, Sigfox, commenced building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far.

Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others.

Energy management

Significant numbers of energy-consuming devices (e.g. switches, power outlets, bulbs, televisions, etc.) already integrate Internet connectivity, which can allow them to communicate with utilities to balance power generation and energy usage and optimize energy consumption as a whole. These devices allow for remote

control by users, or central management via a cloud-based interface, and enable functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). The smart grid is a utility-side IoT application; systems gather and act on energy and power-related information to improve the efficiency of the production and distribution of electricity. Using advanced metering infrastructure (AMI) Internet-connected devices, electric utilities not only collect data from end-users, but also manage distribution automation devices like transformers.

Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource-constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.

IoT ADOPTION BARRIERS

Lack of interoperability and unclear value propositions

Despite a shared belief in the potential of IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Mike Farley argued in Forbes that while IoT solutions appeal to early adopters, they either lack interoperability or a clear use case for end-users. A study by Ericsson regarding the adoption of IoT among Danish companies suggests that many struggle “to pinpoint exactly where the value of IoT lies for them.

Privacy and security concerns

According to a recent study by Noura Aleisa and Karen Renaud at the University of Glasgow, "the Internet of things' potential for major privacy invasion is a concern" with much of research "disproportionally focused on the security concerns of IoT." Among the "proposed solutions in terms of the techniques they deployed and the extent to which they satisfied core privacy principles only very few turned out to be fully satisfactory. Louis Basenese, investment director at Wall Street Daily, has criticized the industry's lack of attention to security issues:

"Despite high-profile and alarming hacks, device manufacturers remain undeterred, focusing on profitability over security. Consumers need to have ultimate control over collected data, including the option to delete it if they choose...Without privacy assurances, wide-scale consumer adoption simply won't happen."

In a post-Snowden world of global surveillance disclosures, consumers take a more active interest in protecting their privacy and demand IoT devices to be screened for potential security vulnerabilities and privacy violations before purchasing them. According to the 2016 Accenture Digital Consumer Survey, in which 28000 consumers in 28 countries were polled on their use of consumer technology, security “has moved from being a nagging problem to a top barrier as consumers are now choosing to abandon IoT devices and services over security concerns.”The survey revealed that “out of the consumers aware of hacker attacks and owning or planning to own IoT devices in the next five years, 18 percent decided to terminate the use of the services and related services until they get safety guarantees.” This suggests that consumers increasingly perceive privacy risks and security concerns to outweigh the value propositions of IoT devices and opt to postpone planned purchases or service subscriptions.

Traditional governance structures

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IoT and companies' traditional governance structures, as IoT still presents both uncertainties and a lack of historical precedence." Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IoT opportunity." This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices. A lack of digital leadership in the age of digital transformation has also stifled innovation and IoT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out", or further action in regards to IoT "was pending competitor moves, customer pull, or regulatory requirements." Some of these companies risk being 'kodaked' – "Kodak was a market leader until digital disruption eclipsed film photography with digital photos"– failing to "see the disruptive forces affecting their industry" and "to truly embrace the new business models the disruptive change opens up." Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in the technology, and even understood that photos would be shared online" but ultimately failed to realize that "online photo sharing was the new business, not just a way to expand the printing business."

Business planning and models

According to 2018 study, 70–75% of IoT deployments were stuck in the pilot or prototype stage, unable to reach scale due in part to a lack of business planning.

Studies on IoT literature and projects show a disproportionate prominence of technology in the IoT projects, which are often driven by technological interventions rather than business model innovation.

IoT SECURITY

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even the radio in your car are signifying a security nightmare being caused by the future of IoT.

When it first appeared, the Internet of Things (IoT) seemed to be nothing more than an idea with no substance. What was it? Was it the new 'IT' (remember that)? Eventually, IoT came to fruition and consumers lapped it up. Smart thermostats, toasters, locks, lighting, Echo, Google Home... the list goes on and on. As more homes and businesses adopt such devices, you can imagine what follows. Security breaches.

Over the last few years, there have been quite a few IoT-centric attacks. And yet despite the attacks on the rise, IoT continues to enjoy an even greater surge in popularity. Should you consider discontinuing the adoption/deployment of IoT devices -- and forego the convenience of tech evolution?

Let's take a look at some of the attacks on IoT devices over the last few years and what you can do to prevent falling victim to vulnerabilities.

1: Stuxnet

We wanted to start off with this particular attack (which occurred between 2010 and 2014), because it perfectly illustrates the inherent danger in IoT devices. Although the devices Stuxnet targeted -- industrial programmable logic controllers (PLCs) -- aren't typical IoT devices per today's standards, they are considered 'smart controllers' and fall into the category. The attack was purportedly launched to sabotage the uranium enrichment facility in Natanz, Iran. Many experts believe that Stuxnet destroyed up to 1,000 centrifuges. Stuxnet was not a typical IoT attack, because it relied on the PLC devices to be connected to a machine running the Windows operating system. Even

so, this should have served as a clear warning sign that smart devices can be compromised.

The lesson to be learned from this attack? Mission-critical devices that rely on a standard PC platform should not be attached to a WAN unless absolutely necessary and need to be safeguarded from access by non-critical personnel.

2: Mirai botnet

The year 2016 had plenty of major attacks to call its own. One such attack was the Mirai botnet. This particular botnet infected numerous IoT devices (primarily older routers and IP cameras), then used them to flood DNS provider Dyne with a DDoS attack. The Mirai botnet took down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites. This piece of malicious code took advantage of devices running out-of-date versions of the Linux kernel and relied on the fact that most users do not change the default usernames/passwords on their devices. It should go without saying that if your IoT device is password protected, you should change the default password (and username, if possible) immediately.

3: Cold in Finland

In November 2016, cybercriminals shut down the heating of two buildings in the city of Lappeenranta, Finland. This was another DDoS attack; in this case, the attack managed to cause the heating controllers to continually reboot the system so that the heating never actually kicked in. Because the temperatures in Finland dip well below freezing at that time of year, this attack was significant.

The lesson learned from this attack? Your network needs to be frequently monitored for DDoS (and other) attacks. The second you see suspect activity on your network... act.

4: Brickerbot

This attack worked in similar fashion to the Mirai botnet, in that it relied upon a DDoS attack and users not changing the default username/password of their device. The biggest difference between

Brickerbot and Mirai botnet is that Brickerbot (as the name implies) simply kills the device. This could be a serious hit on a company's bottom line if a large deployment of IoT devices are rolled out, only to have them simultaneously bricked.

The lesson learned here is that if your devices include a default username/password, you should immediately change them.

5: The botnet barrage

This year, Verizon Wireless released a report that included an unnamed university that saw more than 5,000 IoT devices attacked. When senior members of the campus IT staff started receiving numerous complaints about slow or inaccessible network connectivity, they discovered their name servers were producing a high volume of alerts and showed an abnormal number of sub-domains related to seafood. It turned out more than 5,000 discrete systems were found to be making hundreds of DNS lookups every 15 minutes. The botnet spread via brute force attack to break through weak passwords on IoT devices.

The lesson learned here? Again, always be on the alert for suspect network activity and make sure to secure your IoT devices with stronger than usual passwords.

Shodan

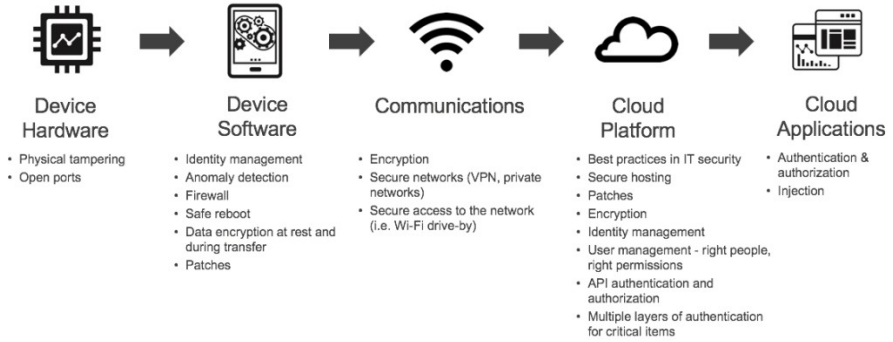
Shodan is a search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites. But what if you're interested in measuring which countries are becoming more connected? Or if you want to know which version of Microsoft IIS is the most popular? Or you want to find the control servers for malware? Maybe a new vulnerability came out and you want to see how many hosts it could affect? Traditional web search engines don't let you answer those questions.

Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary

tremendously: ranging from small desktops up to nuclear power plants and everything in between.

So what does Shodan index then? The bulk of the data is taken from banners, which are metadata about a software that's running on a device. This can be information about the server software, what options the service supports, a welcome message or anything else that the client would like to know before interacting with the server. For example, following is a FTP banner.

HOW TO SECURE YOUR IoT DEVICE ?



INVESTIGATION OF IOT CRIME

THE CHALLENGE OF COMBATING IOT CRIME

Cybercriminals have progressed from targeting computers and networks to people, medical devices, power grids, cars, kitchen appliances and other connected devices. Smart devices are the main components of the IoT. They are easy to use and deploy and are usually connected to the internet without any security enabled. These devices range from smart locks to medical equipment, TVs, refrigerators, light controls, security systems, baby monitors and automobiles, any of which can be used to steal personal information, spread malicious code, eavesdrop or even interfere with the operation of machinery. In a worst-case scenario, these malicious acts can potentially put human lives at risk.

Due to the rising number of connected devices, it has become necessary to develop new approaches and tap all available resources to combat future crimes. This new strategy should be implemented in the early stages of the investigation, particularly when investigators don't know where to begin.

CLASSIFYING CYBERCRIME WITH AN IOT PERSPECTIVE

- ### The IoT as a Target

These crimes are relatively new, which explains why organizations and individuals around the world are largely unprepared to combat them. They are usually committed by a select group of criminals who have the computer skills and scientific knowledge to execute attacks on smart devices. This class of IoT crime involves attackers exploiting vulnerabilities in smart devices, such as pacemakers, medical infusion pumps, smart cars and sniper rifles, and executing malicious instructions that could endanger human life.

- ### The IoT as a Tool

The target of this type of crime is not the IoT device itself, but the smart device used to commit the offense. In this scenario, identifying and prosecuting the perpetrators is more difficult. This class of crime usually requires less technical expertise and depends on manufacturer-introduced vulnerabilities. Since security is typically not the main focus of device manufacturers, IoT devices are perfect tools for attackers to build botnets to execute large distributed denial-of-service (DDOS) attacks. A prominent example is the Mirai botnet, which used connected devices to attack various high-profile technology providers. Attackers typically exploit vulnerabilities such as fixed encryption keys, default passwords and failure to patch or update device firmware.

- ### The IoT as an Eyewitness

These are the crimes that have existed for centuries, such as trespassing, homicide and kidnapping. The only difference here is that these crimes take place in smart environments. Motion sensors,

climate controls and smart-light logs can record the exact time of an intrusion and indicate the intruder's route throughout the house, which can help investigators determine where to look for fingerprints. Smart locks can indicate whether the intruder brute-forced, hacked or leveraged a legitimate code to enter the smart home. Additionally, wireless access points (WAP) may have historical logs of wireless connection attempts and other local WAP activities, which could contain unintentional connection attempts from the intruder's phone.

IoT Forensics

IoT technology is a combination of many technology zones: IoT zone, Network zone and Cloud zone. These zones can be the source of IoT

Digital evidences.

That is, an evidence can be collected from a smart IoT device or a sensor, from an internal network such as a firewall or a router, or from outside networks such as Cloud or an application. Based on these zones, IoT has three aspects in term of forensics: Cloud forensics, network forensics and device level.

Most of IoT devices have the ability to cross Internet (direct or indirect connect) through applications to share their resources in the Cloud. With all valuable data that store in the Cloud, it has recently became one of the most important targets for attackers. In traditional digital forensics, the examiner can hold the digital equipment and then apply the investigation process to extract the evidence. However, in Cloud forensics, it is a different scenario, the evidence could be separated in multi-location which is rising many challenges in terms of acquisition of data from the Cloud. In addition, in the Cloud, examiners have limited control and access to seize the digital equipment and getting an exact place of evidence could be a challenge. Dykstra also addressed this challenge in one of the case study that provided about child pornography website. In the warrant that request the Cloud provider, should provide the name of the data owner, or specify the

location of the data that you are looking for. Besides, data could be stored in a different location in the Cloud, resulting in no evidence could be seized. In addition, as all Cloud services use Virtual Machine as servers, data volatile like registry entries or temporary Internet files in these servers could be erased if they not synchronized with storage devices. For instance, if these servers are restarted or shutdown, the data could be erased.

Network Forensics include all different kinds of networks that IoT devices used to send and receive data. It could be home networks, industrial networks, LANs, MANs and WANs. For instance, if an incident occurs in IoT devices, all logs that traffic flow that has passed throw, could be potential evidence such as firewalls or IDS logs.

Device Level Forensics include all potential digital evidence that can be collected from IoT devices like graphics, audio, video. Videos and graphics from CCTV camera or audios from Amazon Echo, can be great examples of digital evidences in the device level forensics.

IoT forensic Challenges

IoT technology has presented a significant shift in investigation field, especially in how it interacted with data. However, there are some challenges in terms of IoT forensics.

Data Location

Many of IoT data are spread in different locations which are out of the user control. This data could be in the Cloud, in third party's location, in mobile phone or other devices. Therefore, in IoT forensics, to identify the location of evidence is considered as one of the biggest challenges can investigator faced in order to collect the evidence. In addition, IoT data might be located in different countries and be mixed with other users information, which means different countries regulations are involved. A great case example is what was happened in August 2014, when a Microsoft refused to comply with a search warrant that seeking data stored outside the country of war- rant(US), making the case opened for a long period of time.

Lifespan limitation of digital media

Because the limitation of storage in IoT devices, the lifespan of data in IoT devices is short and data can be easily overwritten. Resulting in the possibility of evidence being lost. Therefore, one of the challenges is the period of survival of the evidence in IoT devices before it is overwritten. Transferring the data to another thing such as local Hub or to the Cloud could be an easy solution to solve this challenge. However, it present another challenge that related to securing the chain of evidence and how to prove the evidence has not been changed or modified.

Cloud service requirement

Most of the accounts are anonymous users because Cloud service does not require the accurate information from user to sign up for their service. It could lead to impossible to identify a criminal. For example, even though the investigators find an evidence in the Cloud that prove a particular IoT device in crime scene is the cause of the crime, it does not mean this evidence could lead to identify the criminal.

Lack of Security

Evidence in IoT devices could be changed or deleted because of lack of security, which could make these evidence not solid enough to be accepted in law court. For example, in the market, some companies do not update their devices regularly or at all or some- time they stop supporting the device's framework when they focus on a new product with the new infrastructure. As a result, it could leave these devices vulnerable as hacker found a new vulnerability.

Device type

In identification phase of forensics, the digital investigator needs to identify and acquire the evidence from a digital crime scene. Usually, evidence source is types of a computer system such as computer and mobile phone. However, in IoT, the source of evidence could be objects like a smart refrigerator or smart coffee maker. Therefore, the investigators will face some challenges. One of these

challenging is Identifying and finding the IoT devices in crime scene. It could the device turned off because it run out of battery, which make the chance to be found is so difficult especially if the IoT devices is very small, in hidden place or look like a traditional device. Carrying the device to the lab and finding a space could be another challenge that investigator could face in terms of device type. In addition, extracting the evidences form these devices is considered as anther IoT challenges as most of manufacturer adopts different platforms, operating systems and hardware. One of the examples is the CCTV forensics where the CCTV's manufacturers applied different file system format in their devices. Retrieving properly artefacts from CCTV's storage devices is still a challenges. We also show in a new approach to carve the deleted video footprint a proprietary designed file storage system.

Data Format

The format of the data that generated by IoT devices is not matching to what is saved in the Cloud. In addition, user have no direct access to his/her data and the data presents in deferent format than that in which it is stored. Moreover, Data could be process using analytic functions in different places before be stored in the Could. Hence, in order to be accepted in a law court, data form should be returned to original format before performing analysis.

CONCLUSION

IoT application will resolve below areas and manage our life very fast and easier

- Security
- Autonomy and control
- Social control
- Political manipulation
- Design
- Environmental impact
- Influences human moral decision making

BIBILIOGRAPHY

- *Acharjya, D.P.; Geetha, M.K., ed. (2017).* Internet of Things: Novel Advances and Envisioned Applications*. Springer. p. 311*. ISBN 9783319534725*.*
- *Li, S.; Xu, L.D., ed. (2017).* Securing the Internet of Things*. Syngress. p. 154*. ISBN 9780128045053*.*
- *Rowland, C.; Goodman, E.; Charlier, M.; et al., eds. (2015).* Designing Connected Products: UX for the Consumer Internet of Things*. O'Reilly Media. p. 726*. ISBN 9781449372569*.*
- *Thomas, Jayant; Traukina, Alena (2018).* Industrial Internet Application Development: Simplify IIoT development using the elasticity of Public Cloud and Native Cloud Services*. Packt Publishing. p. 25*. ISBN 978-1788298599*.*

Online banking

TEAM MEMBERS:-

1. SRI. AJMAL KHAN, SI OF POLICE, LAKSHADWEEP
2. SRI. AKHIL D.S, CPO 13098, DHQ ERNAKULAM CITY
3. SRI. SAJIN K.S, CPO 3257, KONNY PS, PATHANAMTHITTA
4. SRI. AJITH, HAV 10472, HI-TECH CELL, TRIVANDRUM
5. SRI. ANEESHCHANDRAN, CPO 6180, HI-TECH CELL, TRIVANDRUM
6. SRI.ANOOP K.N, CPO 6822, HI-TECH CELL, TRIVANDRUM
7. SRI. NIDHIN.R, CPO 7409, KAP 5 BN, KUTTIKANAM
8. SRI. SARATH P NAIR, CPO 7293, DHQ KANNUR
9. SRI. VINEESH M.C, CPO 6817, DHQ KANNUR

Acknowledgment

This Project report on Internet & Mobile Banking is submitted as a part of Advanced Course on Cyber Crime Investigation conducted at PTC, Thiruvananthapuram from 12.09.2018 to 25.10.2018. The Course members were divided into various groups and our group was formed under the leadership of Sri.Ajmal Khan SI of Police from Lakshadweep

We express our sincere gratitude to The Principal, The Vice Principal, Course Coordinators, Indoor and Outdoor Staffs of PTC, Faculties of C-DAC, FSL, and Faculties from various establishments for making us familiar with the Cyber Crime investigation and also giving us valuable directions for completing this project.

INTRODUCTION

INTERNET BANKING

Online banking, also known as internet banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

The customer visits the financial institution's secure website, and enters the online banking facility using the customer number and credentials previously set up.

MOBILE BANKING

Mobile banking is a service provided by a banker or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted.

Transactions through mobile banking may include obtaining account balances and lists of latest transactions, electronic bill payments, remote check deposits, P2P payments, and funds transfers between a customer's or another's accounts. Some apps also enable copies of statements to be downloaded and sometimes printed at the customer's premises; and some banks charge a fee for mailing hardcopies of bank statements.

History of Internet Banking

The evolution process of latest service delivery mechanism through internet i.e. e-banking started from the early 1980s. In late 1980s, the term online got popularized and it was referred to a banking medium of using a terminal, keyboard and monitor to access the

banking system through a phone line. Another term used for this was 'Home Banking' and in it, customers were using a numeric keypad to send tones down a phone line with instructions to the bank. In 1981, e-banking has started in New York with offering home banking service using videotex system by Citi Bank, Chase Manhattan Bank, Chemical bank and manufacturers Hanover bank. Although due to failure of videotex system, Home Banking was not able to gain popularity except in France and UK.

In 1983, Bank of Scotland provided UK's first home online banking service to the banking customers of Nottingham Building Society. This online banking service was based on Prestel system of UK and used a computer like BBC Micro or keyboard connected to the telephone and television system. This system was called Homelink and it enabled customers to view their bank statements online, online fund transfer and online bill payment. To pay bills or transfer funds, customers need to send a written instruction having details of intended transaction to Nottingham Building Society who set the details upon the Homelink system. The usual recipients of this service were electric company, Gas Company, telephone companies and other banks. The account holder has to provide details of the payment through Prestel into Nottingham Building Society system.

Then, a cheque of payment amount has to be send by Nottingham Building Society to the payee and an instruction giving details of the payment was send to the account holder. Later, BACS was used to directly transfer the payment.

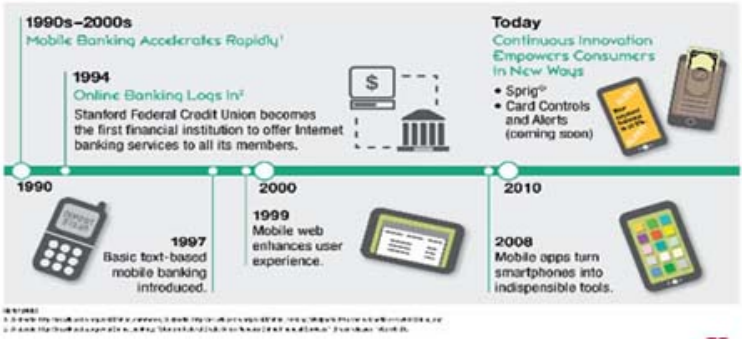
In Oct. 1994, Stanford Federal Credit Union was the first financial institution that provided internet banking facility to its all members. Today, a number of banks are functioning as internet only banks. These internet only banks do not have a physical bank branches

like their predecessors. They differentiate themselves by providing better rate of interest and internet banking facility.

Use of Information & Communication Technology (ICT) is the latest mode of managing data electronically. The advancement of ICT specifically in the utilization rate of internet facility resulted in enhancement of production capacity and increase in fund flow all over the globe. Subsequently, it created a cut throat competitive environment internationally and that lead to challenge of satisfying the customers who are now more aware and educated than earlier. Due to the globalization, the distance between customers and service providers has become irrelevant.

It is well observed that ICT affected the entire financial industry through simplifying enquiry process, better operating speed and providing efficient delivery mechanism for financial services. Same way, banks soon sensed that through adaptation of technological advancements, they can gain competitive advantage.

As the use of computer increasing to improve the operating system in the various sectors of the society, it also provided a new medium to commit crimes for some people. With use of hacking to solve the internet problems in 1960's, computer crimes started and then in 1970s its pace was increased in way of crimes such as privacy



violations, phone tapping, trespassing and distribution of illicit materials. The list of crimes had increased in 1980s by experiencing crimes as, software piracy, copyright violation and introduction of viruses. The scenario became worse and the extent of loss occurred due to these computer crimes is enormous. The international market experienced the same with computers being used for surveillance and transnational organized crime and terrorism.

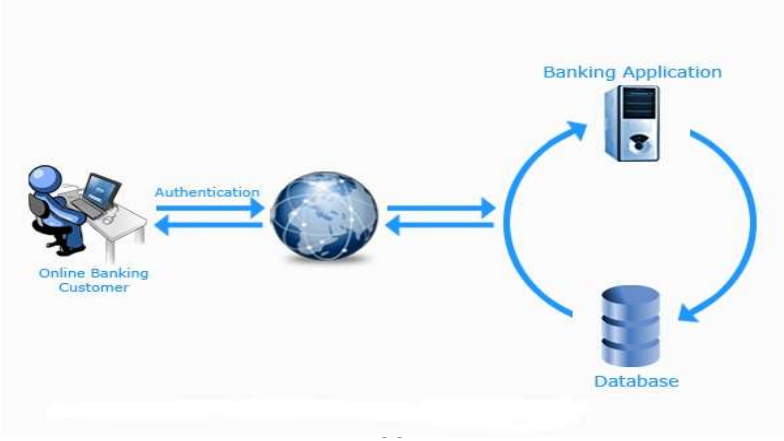
Organizations and banks while starting the computerization phase were not aware about the fact that it would result in fasting the speed of computer crimes. Now, computer becomes a vital part of our life either personal or professional and its use is irrefutable. The working style of banking institutions has completely changed with the use of computer and internet facility. The large number of banking transactions compelled the banks to take the help of computer in processing the transactions. Due to this, the use of computers in internet banking facility become ineluctable.

In essence, computer and the internet facility helps bank to facilitate customers' transactions records and transfer of funds. The computer and internet facility helps customers in various ways as they can directly communicate with the banks, pay their utility bills, transfer the fund, check their account balances and can perform all kind of services offered by their banks. But the use of computer and internet facility provide advantages not only to the banks or organizations but also to the criminally minded people as well.

It is noticeable that even before the occurrence of computer crimes, bank related crimes had occurred. The bank related crimes were bank robbery, false statement to a bank in order to obtain a loan, misapplication or embezzlement of bank fund, false entries in the bank's pass-book, bribery and fraud. There is a significant difference between these traditional bank related crimes and the modern

computer crimes and that is mainly the use of violence in the traditional bank related crimes and the committer of those crimes was more visible and detection of such crime was comparatively easy. Although the characteristics of these crimes are different from each other but the motive behind these crimes are same. The use of computer has provided additional mode and opportunity to such crimes.

In the last thirty years, the financial industry has seen dramatic and revolutionary changes. Globalization, advancement in technology and integration have transformed banking sector in last two decades worldwide and compelled the regulators to deregulate financial system. Deregulation resulted into enhancement of banking customer base, mark-able presence of banks into new markets with modern technologies involved in individual as well as institutional customer interaction. ICT facilitates conventional financial institution to inflate their business to and through internet facility. Additionally, technological advancements reduced the per transaction cost of banks as now there is no need of bank personnel to facilitate customers' bank transaction, it could be self-served through e-banking. The various modes of e-banking, such as, ATMs, Tele- banking, Mobile- banking, debit and credit cards etc.



Internet Banking: Distribution Channels

Today, internet has evolved as the prime medium of service delivery for various financial institutions. Earlier to this, customers were not able to perform their personal and commercial banking transactions with such fast speed as they can perform with internet banking. The internet facility enables banks to perform their traditional activities on a virtual medium, which they use to perform earlier in their branches.

Initially, financial institutions were enthusiastic on identifying advantages of internet and were one of the initiators to adapt e-commerce. After few years down the line, they transformed their websites from only informational websites to dynamic transaction-oriented websites that are providing 'anytime anywhere' banking services.

Besides having a large internet user population, most of banks are still having a wide branch network that delivers same products and services that are provided online as well. Therefore, there must be few opportunities to address this service overlap existed between two kind of distributional channels.

Advantages of Internet Banking

The prime advantage of e-banking system is reduction in operating cost per transaction. Banks can deeply analyze all the information gathered from bank customer interactions with the help of information technology. Therefore, to have effective Customer Relationship Management (CRM) system is become key issue in internet banking services. The effective CRM system enables banks to gain better customer intelligence, precision in customization and better managed customer relationships through their virtual presence. To

enhance its operating efficiency and providing better banking products and services, bank has always been the pioneer in adapting the latest technological advancements. Banks adopted electronic and telecommunication distribution channels for providing various financial services long back. As banks' focus has shifted from product centric model, they have developed their own e-banking system. Now, banks view e-banking which helped in reducing operating cost as an important value added feature to attract and maintain existing and prospecting banking clients.

In India the number of internet users is increasing with very fast pace that eventually increase the opportunity to increase the number of e-banking users as well. But the success of e-banking largely depends on the technological adaptation rate of Indian retail and corporate banking customers. Therefore, the driving forces that influence the adaptation of e-banking system in India will definitely be a critical issue to banks as well as to regulators of the banking industry.

Disadvantages of Internet Banking

Although e-banking system provides a numerous advantages to the customers but still prospecting e-banking users should identify its few disadvantages as well. Even after investing heavily in e-banking awareness campaign and offering so many benefits through e-banking system, still it lacks in gaining trust factor among its customers.

The disadvantages of e-banking system are as follows:

1. Impersonal: Absence of face to face interaction makes it very impersonal. Thus, customers who are more comfortable in dealing with people in physical bank setting that provide those personalised services rather than mechanical interaction; e-banking is not a good option for them.

2. Lack of trust: Still many customers do not trust online mode of service especially for money related transactions. Users who are not seasoned in e-banking feel very uncomfortable as they have doubt regarding the correctness of the transaction done by them online. As they require some kind of proof of transaction as receipt, to verify their transactions.

3. Difficult for first timers: For the beginners, it appears as a complex mode of service as customer find it complicated to navigate through bank's website. While opening an account online, bank's website requires a number of information and that seems time taking and inconvenient process to the first time users.

Challenges of Internet Banking

Indian internet banking sector is still prevailing in its primary level of growth. Only some banks are providing certain basic services only. Only limited number of private sector banks like HDFC & ICICI Bank is fully computerized and they are providing all services through the use of internet. One of the major factors responsible other Indian banks upgrading technology and competing with other competitors is liberalization of the economy.

Challenges of E- Banking are as follows:

1. Demand side pressure due to increasing access to low cost electronic services.
2. Emergence of open standards for banking functionality.
3. Global players in the fray.
4. Dual responsibility, to protect customer's privacy and protect against fraud.
    a) Proper understanding of customer: Bank should adequately and properly identify customers' requirements and wants. To identify the customers exact needs bank should conduct a research survey.
    b) Due to significant increase in customers' awareness, the need of maintaining transparency has increased significantly.
    c) Breach of privacy: While customers conducting banking transactions online, it directly enters into banking records that reveal the identity of customers. Therefore, no one can easily transfer black money.
    d) Bandwidth: Although, internet facility providers claim to provide speedy and high bandwidth, still the problem of high speed internet prevails. E-Banking can popularize more only with adequate infrastructure comprising telecommunication and bandwidth.
    e) The level of computer literacy is still very low in India and it works as a bottleneck in the fast acceptance of e-banking.
    f) The attitude of customers is required to be transformed in India.
    g) Bank should have proper security measures to protect its customers against "net – jacked" or from frauds.

The threats of e-banking are as follows:

1. The most common way of hoaxing with the information is the cracking login and passwords of e- banking users.
2. Denial of services: high trafficking of queries result into jamming computer network.
3. Data Diddling: Information and data can change in an unauthorized way. It can result in receiving higher amount bill rather than actual amount to be paid by customers.
4. Session Hijacking: Hijacker becomes unauthorized intermediary between the customer and the server. Then hijacker can hijack the data and restricts it to reach the relevant destination.

Most online transactions involve disclosing up of the credit or debit card number. Hackers can very easily track down these numbers. They can thus enjoy the full benefits of the card without being an actual cardholder. Reserve Bank of India provided some guidelines on e-banking to protect interest of customers as well as of banks.

To make online banking a safe and secure banking experience you need to follow these steps

- Avoid accessing your account from a cyber café or a shared computer. If you are happen to do so then change your password as soon as you finish your banking transaction.
- Every time you finish using your online banking session then sign out from the site rather then just closing the browser.
- Change your internet banking password after your first login and thereafter regularly.
- Use complex and difficult password and make it difficult for others to guess.
- Use different id and password for different internet accounts.
- Never share your passwords or login details with anybody.

- View your account daily and check it with your transactions, if there is anything which does not tally with your instructions then inform your bank immediately.

The advantages of online banking outnumber its disadvantages and therefore this form of banking has become very popular with the customers. In this modern age of banking, online banking or net banking has made things easier for people and saves lot of time. Though internet banking is the need of every customer, some banks are still not having advance features like transferring money to any bank across the country or easy registration for net banking, this is because some banks are situated in the rural areas where the use of computers is not common. All customers of all banks can be linked by net banking only if technology reaches even the most remote areas of the country.

The guidelines are as following:

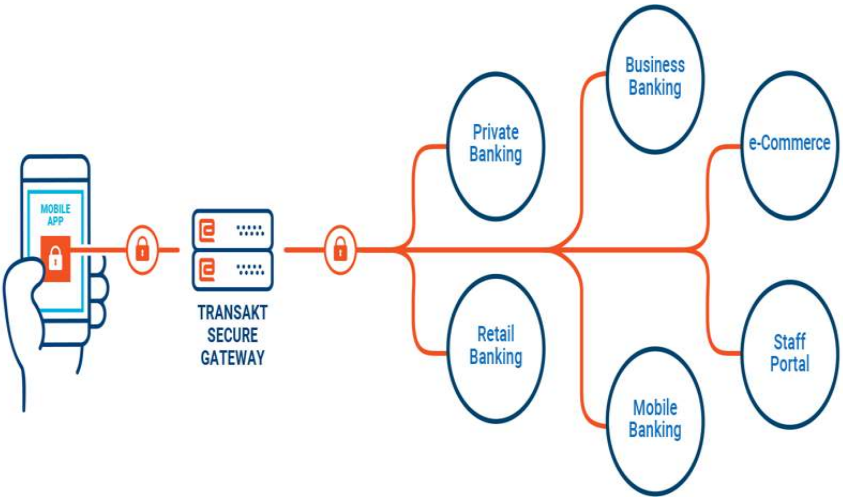
1. It instructed that although banks can accept application of account opening online, but the bank account should be opened after adequate physical verification & introduction of the client.

2. It guided that security measures adopted by bank, for users authentication, must be recognized or approved as a substitute for sign, for legal perspective. As per the IT Act 2000 Sec.3 (2), asymmetric crypto system and hash function tech. should be used as a medium of authentication of electronic records. If bank uses any other medium, it would be taken as a source of legal risk.

MOBILE BANKING

It is a set of applications that enable people to use their mobile telephone to manipulate bank accounts, store value in an account related to their handset, transfer funds or even access credit or insurance products. Its about buying and selling products and services through wireless handheld devices such as mobile phones, or simply saving the money on the handheld.

It is an application that lives on a mobile phone, which access and manipulates their bank accounts at anytime and any where. It is a system that allows customize to perform a number of financial transactions through mobile device. Monitoring our bank accounts through the mobile is known as mobile banking.



Banks Go Mobile

Banks are already investing in mobile technology and security, developing smartphone apps, adding new features such as remote deposit of checks, and educating consumers. Consequently mobile banking adoption among consumers has been much faster than the adoption of online banking more than a decade ago.

Most banks believe that the mobile channel will help them reduce transaction costs as well as increase customer engagement and retention. This is similar to the intended benefits of online banking several years ago. However, a Harvard study shows that while online banking improved customer retention and reduced cost per transaction, it led to an increase in the total number of online and offline transactions that resulted in an increase in the total transaction cost.

More importantly, banks will be myopic if they view mobile as just another channel for doing business. Mobile technology is changing the ecosystem of the banking industry as new players with innovative solutions enter this market. While some players such as Google Wallet are working with existing credit card companies like MasterCard and

Visa, others such as PayPal or Square are emerging as strong competitors that could undermine the traditional partnership between credit card companies and banks.

RBI GUIDELINES

- The guidelines issued by Reserve Bank of India on 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4 February 1998 will apply mutatis mutandis ('the necessary changes having been made') to mobile banking.
- The guidelines issued by RBI on 'know your customer' (KYC), 'anti-money laundering' (AML) and 'combating the financing of terrorism' (CFT) from time to time will be also applicable to mobile-based banking services.
- Banks should offer mobile-based banking service only to their own customers, be it bank account or credit card account holders. However, for the purposes of remittance of funds for disbursement in cash, the receipts could be non-account holder also.
- Banks should have a system of document-based registration with mandatory physical presence of their customers before commencing mobile-banking service.
- There can be two levels of mobile-based banking service. The first level is in the nature of information like balance enquiry, SMS alert for credit or debit, status of last five transactions, and many other information-providing services. The account-opening form, at the time of opening new bank account, should clearly indicate the option for 'mobile banking'.

- The second or standard level of mobile-banking services could involve financial transactions such as payments, transfers and stop payments. Banking transactions up to Rs:5,000 can be facilitated by banks without end-to-end encryption.
- Banks are permitted to offer mobile-banking facility to their customers without any daily cap for transactions involving purchase of goods/services.
- In case of cash-out, the maximum value of such transfers shall be Rs:10,000 per transaction. Banks may place a suitable cap on the velocity of such transactions, subject to a maximum of Rs:25,000 per month per beneficiary.
- Banks are required to maintain security and confidentiality of customers' accounts since in the mobile banking scenario the risk of banks not meeting the above obligation is high.
- Banks are required to make mandatory disclosures of risks, responsibilities and liabilities of the customers on their websites and/or through printed material.
- Banks may carry out due diligence of the persons before appointing them as authorized agents for such services. Banks shall, however, be responsible as principals for all the acts of omission or commission of their agents.
- The existing mechanism of handling customer complaints/ grievances may be used for mobile-banking transactions as well. However, in view of the fact that the technology is relatively new, banks should set up a help desk and disclose on their websites the details of the help desk and escalation procedure for lodging complaints. Such details should also be made available to the customers at the time of sign-up.
- In cases where the customer files a complaint with the bank disputing a transaction, it will be the responsibility of the service-providing bank to address the customer grievance. Banks should formulate charge-back procedures for addressing such customer

grievances. The grievance-handling procedure including the compensation policy should be disclosed.

- Customers' complaints/grievances arising out of mobile-banking facility will be covered under the Banking Ombudsman Scheme.

Security Tips

- Most of the phones support numeric password lock. Activate one for your phone with a password that is difficult to crack. Avoid using your or any of your family members' birth or anniversary date as well as house car or phone numbers. (Most mobile and internet banking frauds, as per government records, are committed by the people known to you.)
- If you own a smartphone, install applications that can protect passwords and cannot give access to your bank even if the phone is stolen. Ideally, the thief should not be able to access any information stored in your phone.
- Never save your ATM pin or your one-time transaction password (OTP) in the phonebook. Even if you do, disguise it as a 10-digit number to make it look like a phone number (with a fake name in the phonebook).
- Never disclose your personal information such as account number, password and PAN card number in text messages.
- Always keep your phone's Bluetooth turned off and do not accept data from unknown sources. Wi-Fi access in public places might have virus and malware that can attack phones. Install credible antivirus on phone to protect it from attacks.

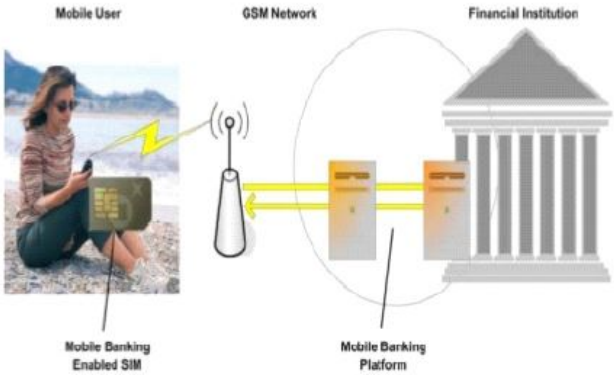
- Delete your 'bank balance' messages from your phone immediately after reading.
- Avoid opening unknown Web links/spam emails on your phone. Also avoid downloading applications that do not come from credible developers.
- Often change your account passwords at random intervals
- Avoid keeping same passwords for all your bank accounts.

MOBILE BANKING SERVICES

Typical Mobile Banking services may include.

- Balance Enquiry
- Mini Statement
- Check Status
- Check Book Requests
- Fund Transfer between account
- Credit/Debit Alerts
- Minimum Balance Alerts

WORKING OF MOBILE-BANKING



LEGAL RELATION OF E-BANKING IN INDIA

Law cannot possibly be expected to keep pace with changes in technology. The recent debacle of virtual voyeurism has brought out, amongst other things, the inadequacy and vulnerability of the laws governing use of internet. Fixing liability, recording and reproducing evidence, ascertaining jurisdiction are problems which show little sign of easing. Concerns over security and misuse pertaining to e-banking activity have been mounting as more banks in India foray into electronic banking.

Though there was a message to banks that they should be formed for public good, since inception, banking has always been a commercial venture, the prime motive of banks being to enlarge profits. And lately adoption of new economic environment such as liberalisation, privatization and globalization has caused concern in banking sector. Indian banks have also undergone a sweeping change where deregulation, technological innovations and globalization are significantly affecting the banking services.

The emergence of internet banking has made many banks to rethink their Information Technology (IT) strategies in competitive markets. It is suggested that the banks that fail to respond to the emergence of internet banking in the market are likely to lose customers and that the cost of offering internet banking services is less than the cost of keeping branch banking.

India has great prospect compared to other developing nations to leverage the potential of E-Banking and build a cash light economy. In addition to IT edge and relatively dense population, the Government of India (GOI) has clearly determined to achieve financial inclusion4 and is taking aggressive steps to see this happens. Rendering financial services to the un-served or poor through a market led approach is important for sustainability of financial inclusion.

There are many reforms and enrolment drives which have been undertaken by the Reserve Bank of India (herein referred as RBI) and GOI in matter of financial inclusion over the last decade. The RBI

and GOI policy initiatives and reforms have considerably helped the development of E-Banking system. The reforms include adoption of technology prototypes like smart cards, mobile based options, debit cards and credit cards. These facilities and advancement have given vent to more market driven environment, which is in fact, the future face of the Indian economy.

Adoption of new technology has resulted in risks6. The legal risk is one which arises from violation of, or non-conformance with laws, rules, regulations, prescribed practices, or when the legal rights and obligation of the transaction are not based on well established norms. Given the relatively new nature of internet banking, rights and obligations in certain cases are uncertain and applicability of laws and rules is also ambiguous. Other reason for legal risks is also uncertainty about the validity of agreements formed via electronic media and law relating to customers disclosure and privacy protection. A customer, who is inadequately informed about his rights and obligation, may not take proper precaution while using internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory authority. Legal risk is directly related to the electronic banking and they increase as and when its use is extended. They mainly stem from the uncertainty that exists in the legal and regulatory framework concerning E-Banking. In most countries an explicit regulating framework does exist and this is due to the experience they had in the sector of E-Banking. But the problem arises when there is no regulatory framework, where a banker offers its electronic services to other countries as well, and unified legal frame in international level does not exist.

Moreover, there is another legal risk which is relating to protection of the customers privacy. Bad use of the technology by the bank personnel or by exterior malignant intruders can expose a bank in a serious legal risk such as fraud, misrepresentation and misappropriation of funds. It is possible that the intruders acquire access in the databases of the banks and use the data of customers in order to commit fraud. In the enthusiasm of enhancing customer

service, bank may link their internet site to other site also. This may cause legal complications and risk. Further hackers may use the linked site to defraud a bank's customer. If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risk. With the introduction of E-banking, digital signatures are also recognized. A digital certificate is granted by the certification authority which ensures that a given signature is, in fact, generated by a given signer. If any fraud takes place the certifying bank may become liable for financial losses incurred by the party who has relied on the digital certificate.

To cope with the risks on one hand and pressure of growing competition on the other has become inevitable to Indian banks. The banks have adopted several initiatives to curb the risk and also to play a safe in the competition world. The competition has been especially tough for the public sector banks (PSBs), as the newly established private sector and foreign banks have already sharpened their competitive edge. Some of the proactive PSB's have been striving hard to make their structures flexible enough to accommodate technological changes.10To regulate the banking in India there are many statutes, which forms the legal framework such as *Banking Regulation Act, 1949,11 The Reserve Bank of India Act, 1934,12 The Negotiable Instruments Act, 1881,13 The Indian Contract Act, 1882,14 Foreign Exchange Management Act, 1999,15 Consumer Protection Act, 1986,16 Prevention of Money Laundering Act, 2002,17 Bankers Books Evidence Act, 1891,18Indian Evidence Act, 1872,19Indian Penal Code, 1860,20 The Payment and Settlement Systems Act, 2007*21 and most importantly *Information Technology Act, 200022* to look into crimes committed due to E-Banking.

E-Banking is an extension of traditional banking services with technology. As technology continues to advance, security measures also continue to improve and become more sophisticated. In 1994, Saraf Committee was appointed to study and recommend on technological issues relating to Electronic Fund Transfers (EFT). The following recommendations were made by the committee.

1. Establishment of an EFT system, with the BANKNET communications network as its carrier.
2. Enactment of suitable legislation on the lines of the Electronic Funds Transfer law.
3. Magnetic Ink Character Recognition clearing is to be introduced.
4. Introduction of Electronic Clearing Service Credit for low value repetitive transactions such as interest, dividend, salary, pension payments and an Electronic Debit Clearing for payments to utility companies.
5. Large scale induction of computers and communication technology inservice branches.
6. Promotion of a card culture, as well as enhanced training facilities.

Many of these recommendations were implemented by the RBI. In 1998, Narasimhan committee was formed which made certain recommendation for the implementation EFT in Indian banking sphere.

- Encryption on Public Switching Telephone Network (PSTN) lines.
- Admission of electronic files as evidence.
- Treating Electronic Funds Transfers on par with crossed cheques/drafts for purposes of Income Tax etc.
- Electronic Record keeping.
- Provide data protection.
- Implementation of digital signatures.
- Clarification on payment finality in case of EFT.

The *Information Technology Act, 2000* (herein after referred as IT Act, 2000) has attempted to address a number of E-Commerce regulatory issues. The law was amended in 2008 based on the recommendation of the 'Working Group on Internet Banking' which examines three thrust areas such as technology and security issues, legal issues and regulatory and supervisory issue. Some of the recommendations have been addressed in the IT amended Act, 2008.

It is the legal department in the bank which is entrusted with the function to advice the business groups on the legal issues arising out of the use of IT.

Law Relating to E-Banking in India

Law relating to banking in India has undergone sweeping changes after the advent of technology. The changes have been made due to revolution in banking sector worldwide. To meet the international standard in service the transformation was necessary. There are amendments carried to the existing laws to meet the needs of the technology in banking.

Reserve Bank of India Act, 1934

In 1995, the Reserve Bank had set up the Committee for Proposing Legislation on Electronic Funds Transfer and other Electronic Payments. Based on the recommendation, the *Reserve Bank of India Act, 1934* (herein after referred as RBI Act, 1934) was amended to include electronic banking operation. A new clause to section 58, sub-section 2 of the Act, relating to the regulation of funds transfer through electronic means between banks, i.e transactions like Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT) and other funds transfer was inserted, to facilitate such EFTs and ensure legal admissibility of documents and records. RBI encouraged electronic payment system has introduced Electronic Clearing Service (ECS) and EFT system in 1995, the RTGS system in 2004, NEFT system in 2005 and Cheque Truncation System (CTS) in 2008.ECS is an electronic mode of payment / receipt for transactions that are repetitive and periodic in nature. ECS is used by institutions for making bulk payment of amounts towards distribution of dividend, interest, salary, pension, or for bulk collection of amounts towards telephone / electricity / water dues, cess / tax collections, loan instalment repayments, periodic investments in mutual funds, insurance premium and other receipts. Essentially, ECS facilitates bulk transfer of money from one bank account to many bank accounts or vice versa. ECS and EFT was introduced in the year 1995, RTGS was introduced in 2004 and NEFT

was introduced in 2005 by amending RBI Act. System of truncation of cheques was also recognized by the RBI. Truncation is the process of stopping the flow of the physical cheque issued by a drawer to the drawee branch. The physical instrument will be truncated at some point en-route to the drawee branch and an electronic image of the cheque would be sent to the drawee branch along with the relevant information like the MICR fields, date of presentation, presenting banks etc. Thus with the implementation of cheque truncation, the need to move the physical instruments across branches would not be required, except in exceptional circumstances. This would effectively reduce the time required for payment of cheques and the associated cost of transit and delay in processing, thus speeding up the process of collection or realization of the cheques. CTS was introduced in 2008. Working group was constituted headed by Shri. G. Gopalakrishnan to study frauds due to electronic banking which gave its report. In the Report the committee has highlighted the danger of compliance or checklist type of mind set and called for dynamic and proactive assessment of various threats and their mitigation. One of the important aspects is the focus on “information security awareness”, as it is acknowledged that people often represent the weakest link in the security chain. In addition, the Report has called for enhancing the use of technology for identifying anomalous e-banking transactions, effective analysis of audit trails and logs, enhancing audit processes through the use of computer assisted audit tools, identifying vulnerabilities in systems and networks and using application systems for carrying out critical business processes involving financial/regulatory/legal and customer related implications rather than through manual methods or through spread sheets. Meanwhile RBI has issued guidelines on Security Issues and Risk mitigation measures related to Card Present (CP) transactions. The highlights of this circular is measure has been taken to secure Card Not Present (CNP) transactions, making it mandatory for banks to put in place additional authentication/validation for all on-line recurring transactions based on information not available on the credit/debit /prepaid cards. Accordingly, banks and other stakeholders are directed

to initiate immediate action for accomplishing the following tasks within the time indicated. Implementation of improved fraud risk management practices and securing the technology infrastructure were the task assigned to the commercial banks in India. The target time given for the completing of the task was September, 2012. With the *Banking Laws Amendment Act, 2012*, RBI is empowered to call for any information and cause inspection of business of any 'associate enterprise' of a bank. This has provided legal framework for setting up a Bank Holding Companies and paves the way for issue of new bank licenses. RBI has been issuing guidelines to the commercial banks on IT, electronic banking and technological risk management and cyber frauds.

Banking Regulation Act, 1949

The Act originally came into force on 16th March, 1949 and it was known as *Banking Companies Act, 1949*. It was amended was renamed as *Banking (Acquisition and Transfer of Undertaking) Act, 1969* and the original Act was extended to the cooperative banks from 1966 and is simply called as B.R.Act, 1949. The objectives of the Act are, to safeguard the interest of depositors, to develop banking institutions on sound lines and to attain the monetary and credit system to the larger interests and priorities of the nation. Amendment has been brought to the original legislation as regards acquiring of shares. An approval may be granted by the RBI if it is satisfied that the shares are acquired in the interest of public, or the in the interest of banking policy or to prevent the affairs of any banking company being conducted in manner detrimental to public interest or companies interest, or in the interest of the emerging trends in banking and international practices, or in the interest of banking and financial system in India.

The applicant is the proper person to acquire shares or voting rights and no other person has such right. The voting right given under the law has immense power to the shareholders to control the banking business of the company.

The RBI has exclusive power to issue, accept or reject application for licence to carry on banking business. The RBI shall establish a Fund to be called the "Depositor Education and Awareness Fund". The salient features of the *Banking Laws (Amendment) Act, 2012*38 are-

1. Regulatory power to supersede board of banks

Under the *Banking Regulation Act, 1949* (herein after referred as B R Act, 1949) the RBI could remove a director or any other officer of the bank. RBI is empowered to supersede the board of directors of a bank for up 12 months if it feels that the board is not working in the interest of shareholders and depositors'. In case the bank is not working in the interest of the shareholders or depositors, RBI shall carry on the business of the bank by appointing an administrator during the period. RBI now being armed with powers to supersede the Board, it can now effectively influence and regulate management of banks. To limit arbitrary exercise of power by the RBI, the Act provides for consultation with the Indian Government.

2. Inspect associate enterprises

The Act empowers the RBI to call for any information and cause inspection of business of any 'associate enterprise' of a bank. This should provide legal framework for setting up of Bank Holding companies and pave the way for issue of new bank licenses. Associate enterprises could be a holding company or subsidiary company of the bank, a joint venture, an enterprise which controls the composition of the Board of Directors of the bank, an enterprise which influences the bank in taking financial decision or an enterprise which obtains economic benefits from the activities of the bank.

RBI may not be able to call for information from 'associate enterprises' incorporated outside India of foreign banks. However, the Indian branches and Indian associate enterprises of a foreign bank will fall under the RBI purview of 'associate enterprise' and they may call for information. An associate enterprise (outside India) of a foreign bank which has a Wholly-Owned- Subsidiary (WOS) in India is covered under the Act.

3. Increase in voting rights

In a public sector bank (PSB), no shareholder (except the Central Government) shall exercise voting rights in excess of one percent of the total voting rights of all the share holders. Further, the preference share holder (except the Central Government) also has an embargo on the voting rights up to one percent of total voting rights of all the shareholders holding preference share capital only. The Act raises the shareholders' voting rights in a public sector bank from one percent to 10 percent. No shareholder, in a private sector bank, can exercise voting rights in excess of ten percent of the total voting rights of all the shareholders.

4. Conversion of a branch of a bank into Wholly Owned Subsidiary

Conversion of a branch of any bank into a Wholly Owned Subsidiary (WOS) or transfer of shareholding of a bank to its holding company is now exempt from stamp duty. These amendments would be beneficial for various stakeholders in the banking sector. While the banking regulator gets enhanced powers that will result in effective compliance of regulations, banks will be able to attract more investments to raise funds for business expansion and to meet capital norms. Accounts and audit, is also very strict under the law. It is the auditor who should examine whether there is an effective system of obtaining confirmations/acknowledgement of debts periodically. For this purpose, the auditors should also review the branch audit reports. The auditor is expected to report on the following aspects of the recovery period, existence of a recovery policy, regular updating, monitoring and adherence, compliance with the RBI guidelines and system of monitoring of recovery from credit card dues in respect of credit cards issued.

The auditor is expected to give his observations on major frauds discovered during the year under the audit. The auditor is also expected to comment on the efficacy of the system and follow up on vigilance reports. According to R.B. Burman Committee recommendation the bank and financial institutions should conduct

Information System Audit conforming to information system audit policy, which has been incorporated in the present system.

Negotiable Instruments Act, 1881

Under the *Negotiable Instruments Act, 1881*, cheque44 includes electronic image of truncated cheque and a cheque in the electronic form. The definition of a cheque in electronic form contemplates digital signature with or without biometric signature and asymmetric crypto system.

Cheque truncation, loosely defined, is the process in which the physical movement of cheque within bank, between banks and clearing house is curtailed or eliminated, being replaced in whole or in part, by electronic records of their content, with or without images, for further processing and transmission.

The truncation of cheque in clearing has been given effect to and appropriate safeguards in this regard have been put forth in the guidelines issued from time to time. Cheque Truncation speeds up the process of collection of cheques resulting in better service to customers reduces the scope for clearing-related frauds or loss of instruments in transit, lowers the cost of collection of cheques, and removes reconciliation-related and logistics-related problems, thus benefitting the system as a whole.

The truncated cheque is an electronic image of the cheque. When it is presented for payment, the draw bank is entitled to demand any further information regarding the truncated cheque from the bank holding the truncated cheque in case of any reasonable suspicion about the genuineness of the apparent tenor of instrument and if the suspicion is that of any fraud, forgery, tampering or destruction of the instrument, it is entitle to further demand the presentment of the truncated cheque itself for verification, provided that the truncated cheque so demanded by the drawee bank shall be retained by it, if payment is made accordingly. This provision protects the paying banker who pays in good faith and without negligence.

Truncation of cheques can be done by the clearing house or the bank which collects the truncated version of the cheque. As per Section 81 of the NI Act, the banker who receives the payment is also supposed to retain the copy of the cheque even after payment has been done. Section 89 of the NI Act says that any distinction between the original cheque and the truncated image should be construed as material alteration.

A material alteration is one which varies the rights, liabilities, or legal position of the parties ascertained by the deed in its original state or otherwise varies the legal effect of the instrument as originally expressed, or reduces to certainty some provision which was originally unascertained and as such void, or may otherwise prejudice the party bound by the deed as originally executed. In such cases it is obligatory on the part of the clearing house or the bank to ensure the correctness of the truncated image while transmitting the image.

The Supreme Court of India has opined that there should be early disposal of cases relating to dishonour of cheques, enhancing punishment for offenders, introducing electronic image of a truncated cheque and a cheque in the electronic form as well as exempting an official nominee director from prosecution under the NI Act, 1881.A certificate issued on the foot of the printout of the electronic image of a truncated cheque by the banker who paid the instrument, shall be *prima facie* proof of such payment. Where the cheque is an electronic image of a truncated cheque, any difference in apparent tenure of such electronic image and the truncated cheque shall be a material alteration and it shall be the duty of the bank or the clearing house, as the case may be, to ensure the exactness of the apparent tenure of electronic image of the truncated cheque while truncating and transmitting the image. Any bank or a clearing house which receives a transmitted electronic image of a truncated cheque, shall verify from the party who transmitted the image to it, that the image so transmitted to it and received by it, is exactly the same. NI Act makes an obligation on the banks to make payment in due course Section 131 of the *Negotiable Instruments (Amendment and Miscellaneous*

Provisions) Act, 2002) Act57 has an explanation which states, 'it shall be the duty of the banker who receives payment based on an electronic image of a truncated cheque held with him, to verify the *prima facie* genuineness of the cheque to be truncated and and any fraud, forgery or tampering apparent on the face of the instrument that can be verified with due diligence and ordinary care'. In case of dishonor of cheque, the period for giving notice of dishonour has been extended to 30 days instead of 15 days. Also any dispute in this matter shall be resolved within 2 years (instead of 1 Year) from the date of institution of the suit.

Truncating cheques entails additional operational risks. Banks have to take adequate measures to ensure that all necessary safeguards are provided. It must be in consonance with the legal requirements and banking practice. While making payment especially of high value instruments under the system extra care has to be taken, otherwise the banker will become liable under section 131 of the NI Act. But a clearing house cannot be held liable for fraud or forgery, as they cannot open the truncated cheques. In all cases the banker should act judiciously and within the purview of the law.

Bankers Books Evidence Act, 1891

Amendment is carried even to the *Bankers Books Evidence Act*, after the advent of E-Banking in India. Section 2 of the Act defines which books are 'bankers books'. This includes ledgers, day-books, cash-books, account-books and all other records used in the ordinary business of the bank, whether these records are kept in written form or stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism, either onsite or at any offsite location including a back-up or disaster recovery site of both. And a printout of any entry in the books of a bank stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such printout as a copy is admissible as evidence.

Certified copy means books in written form and has an attestation as 'true copy' and printout or data stored in a floppy, disc, tape or any other electronic magnetic storage system. The printout shall have certificate of bank manager and computer in-charge person. All these amendments have made the law applicable to cases relating to E-Banking when evidence is produced before the court of law or an arbitrator.

Prevention of Money Laundering Act, 2002

Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy. Money laundering is defined as the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income.

Every financial institution is charged with the responsibility of developing policies and procedures to combat money laundering, which includes the duty to be aware of trends and adaptations in the methods by which money laundering is carried out. The most difficult aspect of this responsibility is a financial organisation's ability to anticipate new criminal behaviour and to proactively implement protocols before the criminal behaviour occurs.

Bankers play the most prominent role and without their connivance the operation on money laundering cannot be curtailed. Development of new high-tech coupled with wire transfer of funds has further aggravated the difficulties to detect the movement of slush funds.

As internet banking transactions are conducted remotely, banks may find it difficult to apply money laundering rules for some forms of electronic payments.

Thus, banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with 'know your customer' (KYC) rules. Every banking company, financial institution and intermediary, as the case may be, is required to maintain a record of transactions as prescribed by the rules and furnish information to the director within time prescribed under the law. The principal officer of the financial institution should furnish the information in writing or by fax or e-mail to the director. The records to be maintained by such entities are set forth in rule 3 of PMLR. Such records include record of cash transactions of value more than ten lakhs or its equivalent in foreign currency. Integrally connected cash transaction which takes place within one month, of any forged or counterfeit note, or there is any suspicious transactions should also be reported every month before 15th day of the succeeding month. Such records are to be maintained by the financial institutions for ten years from the date of the transaction. The financial institution is also required to maintain the records and identity of their clients.

The financial institution is required to formulate and implement a client identification programme and for this they may have their own additional requirements to determine the identity of the clients. A copy of the said identification programme is required to be forwarded to the director. The above provision needs to be appreciated, though they are procedural in nature, it leads to maintenance of records and reporting of transactions which helps in tracking frauds, forgeries and money laundering and the persons involved in such transactions.

The law is a penal law. It imposes penalty for every failure. This penalty may in addition to penalties imposed by other laws. The officer in charge of and responsible to the conduct of the business shall be liable to be prosecuted and punished under this Act. It is therefore

clear that such entities should have a robust system of keeping track of the transactions of the nature referred in the Act and the Rule and report the same within the prescribed period to the authority concerned. The fear to the financial institution is not just penalty, but reputation risk of the entity.

Information Technology Act, 2000

This is the pivotal legislation dealing with crimes committed due to technology in India. Technological innovation in general and IT applications in particular, have had a major effect in banking and finance.

The technology and security standards are of prime important as the entire base of Internet banking rests on it. If the technology and security standards are inadequate, then Internet banking will not provide the desired results and will collapse ultimately. The adoption of firm's available new technology has been recognized as an important part of the overall process of technological change. Information security is concerned with the protection of three characteristics of information, confidentiality, integrity and availability through the use of technical solutions and managerial actions. The IT Act 2000 was amended in 2008 enlarging definitions, introducing the concept of electronic signature, creating new offences, and many more things. IT Act, 2000 had only two sections dealing with computer related offences generally.

The amended Act provides for a stronger data protection measures as well as strengthening the general framework against cybercrimes. There are certain issues which are inherent in the very nature of crimes committed by using IT which are specifically applicable to banker and customer. They are anonymity in cyberspace, the issue as to jurisdiction, the question of reliability and procuring of evidence and the issue of non-reporting of cybercrimes to authorities due to the bad publicity to the business. The issues that are specific to banker and customer, apart from the above, are enlisted below-

1. Intermediary

From times immemorial banker and customer relationship consisted of multiple roles such as debtor and creditor, agent and principal, bailor and bailee, trustee and beneficiary, which were called as general and special relationship between banker and customer. With the innovation in technology and adoption of it by the banker has created a new role to the banker as 'intermediary' and in certain respect as a 'data/information owner'.

The definition of 'intermediary' under IT Act, 2000, means 'any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message'. Though the banks are not directly referred to in the definition, the term is very wide to cover the banker, as the banker receives payments on behalf of the customers by receiving electronic messages. The same procedure applies for making payments on behalf of the customer which are normal activities of the banker.

This renders them as intermediaries. Further, the definition also covers any person who provides any service with respect to such messages/records, in which case it is possible that banks may fall within the definition of the term 'intermediary'.

The definition was amended in 2008. The amended definition reads intermediaries as 'intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service 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'. The amendment does not really change the position of banks as intermediary but now even electronic records maintenance and transmission makes banks as intermediaries for E-Banking.

The IT Act places some responsibilities on intermediaries such as secure the E-Transactions, password and pay with due diligence. In

Sanjay Kumar Kediav. Central Bureau and Anr, Supreme Court held that the service providers (intermediaries) are not liable for act done with due diligence. Whatever it is, uncertainty whether banker is an intermediary or not is not in the interest of the customer. Only thing is banker should act judiciously in case of E-Banking transaction.

2. Encryption

The Central Government may, for securing the use of the electronic medium and for promotion of E-governance and E-commerce, prescribe the modes or methods for encryption. This is because any data which is transferred online is subject to the risk of being intercepted and misused. Encrypting data before transferring it over the internet will go a long way in safeguarding against such interception. But such interception will not be of any use unless it is decrypted. If encryption of data is adopted by internet service providers, it will be helpful in protecting the customers' privacy and also protection of all other data's. Internet Service Provider licence restricts the level of encryption for individuals, groups or organizations. For banks RBI has stipulated a Secure Sockets Layer (SSL).

3. Data Protection

Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize intrusion into ones privacy caused by the collection, storage and dissemination of personal data. Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency.

IT Act imposes civil and criminal liability on a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected.

It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such

circumstances. It is in the discretion of the court to grant compensation to the victim. The Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any electronic record and information without the consent of the person concerned discloses such information to any other person, then he shall be punished with imprisonment upto two years or with fine upto one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of powers granted under IT Act, 2000. As of now, the issue of data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms personal data, personal sensitive data, data which may not be transferred out of or to India and mode of handling the same. Many a time the data is leaked or fraud is carried with the help of employee of the bank also.

Internal threats can stem from three areas: the application development department, the infrastructure, and the data center. Despite the risk of internal threats, it is highly believed that threats from employees are largely unintentional. Threats from the employees results in misappropriation and embezzlement of funds.

4. Computer related offences and Penalty/Punishment

The IT Act, 2000 as amended, exposes the banks to both civil and criminal liability. The civil liability could consist of exposure to pay damages by way of compensation upto five crores under the amended IT Act before the Adjudicating Officer and beyond five crores in a court of competent jurisdiction.

There could also be exposure to criminal liability to the top management of the banks given the provisions of Chapter XI of the amended IT Act and the exposure to criminal liability could consist of imprisonment for a term which would extend from three years to life

imprisonment as also fine. Phishing is one such offence which is covered.

5. Bank's to be licensed as Certifying Authority

Banks shall be allowed to apply for a license to issue digital signature certificate and function as certifying authority for facilitating Internet banking and that Reserve Bank of India shall issue the licence under clause (o) of Section 6(1) of the Banking Regulations Act, 1949.

The authentication of electronic records for the purposes of Internet banking should be in accordance with the provisions of the Act. The electronic records duly maintained for the purposes of Internet banking would be recognized as legally valid and admissible.

The digital signature affixed in a proper manner would satisfy the requirement of signing of a document for the purposes of Internet banking. A digital signature meeting the specified requirements would be deemed to be a secured digital signature for carrying out Internet banking transactions.

Digital signatures share some interesting features with legal signatures in the sense that they can be fairly readily and intimately related to an individual and they serve to authenticate digital content with a high degree of assurance. Any kind of paper work, which is required to be filed in the government offices or its agencies, would be deemed to be duly filed if it is filed in the prescribed electronic form.

Thus the paper formalities can be effectively substituted with electronic filings for Internet banking purposes. The records are maintained in electronic form. And then each bank can also publish rules, regulations, order, bye-laws, notification or any other matter pertaining to its business in electronic format.

If electronic record is sent by the originator or by his agent or by an information system programmed by or on behalf of the originator to operate automatically, then the electronic record shall be attributed to the originator. The requirement of acknowledgement of documents sent for the purposes of Internet banking is adequately safeguarded by the Act. The Internet banking may require to determine

the time and place of dispatch and receipt of electronic records. The Internet banking would require the secured electronic records for its proper working. Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. The CG has the power to prescribe the security procedures to give effect to the provisions of the Act, having regard to the commercial circumstances prevailing at the time when the procedure was used. Thus, the CG can specify safety measures and security procedures for Internet banking under the provisions of the Act. The Controller of Certifying Authorities can issue licenses to the Certification Authority under the IT Act, 2000. The Certifying Authority is assisted by the Registration Authority, which is created at the level of the organizations subscribing to the services of the Certifying Authority. The Reserve Bank would function as a Registration Authority for the proper functioning of Internet banking. Thus, the IT Act, 2000 has laid down the basic legal framework conducive to the Internet banking in India. It must be noted that the object of the Act is to facilitate e-commerce and e-governance, which is essential for the functioning of the internet banking.

Table showing Offences and Punishment under IT Act, 2008 with regards to crimes against Electronic Banking

Section	Particulars	Punishment
Section 43	If a person without the permission of the owner or anyone in charge of a computer system or network, secures access to such computer, downloads, copies or extracts data stored therein, introduces viruses or contaminants into the system, damages and/or disrupts the computer system, denies access to a person authorized to access the computer, tampers	He shall be liable to pay damages by way of compensation to the person so affected.

	with the computer system, destroys, deletes or alters information in a computer system,	
Section 66 B	Receiving a stolen computer resource.	Up to 3 years imprisonment, fine up to Rs 1 lakh or both.
Section 66 C	Identity theft	Up to 3 years imprisonment, fine up to Rs 1 lakh.
Section 66 D	Cheating by impersonation	Up to 3 years imprisonment, fine up to Rs 1 lakh
Section 66 E	Violation of privacy, video voyeurism.	Up to 3 years imprisonment, fine up to Rs 2 lakhs or both.
Section 66 F	Cyber Terrorism	Life Imprisonment.
Section 67	Publishing or transmitting obscene material in electronic form.	Up to 10 years imprisonment with fine up to Rs.2 lakhs
Section 71	Misrepresentation and Suppression of material facts	Up to 2 years imprisonment with fine of Rs. 1 lakh or both.
Section 74	Publication for fraudulent purpose	Up to 2 years imprisonment with fine of Rs. 1 lakh or both
Section 85	Criminal liability of top bank management for various computer related offences	Minimum 3 years imprisonment and maximum life imprisonment

Apart from the above, the following important sections have been substituted and inserted by the IT Amendment Act, 2008:

Section 67 C – Preservation and Retention of information by intermediaries –

This is related to matter for storing information in electronic form. Banks as intermediaries are required to store electronic information for some time as prescribed by RBI and report the same in its audit report.

Section 69 and 69 A– Powers to issue directions for interception or monitoring or decryption of any information through any computer resource – If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

Section 69 B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

The cyber police or investigating authority has been authorized to collect data or information that is necessary to monitor the flow of data within or outside the country. Banks have to provide the same to the authority whenever called for.

Section 72 A – Punishment for Disclosure of information in breach of lawful contract- The person disclosing shall be punished with imprisonment for a term which may extend to two years, or with fine up to one lakh rupees, or with both.

Section 79 – Exemption from liability of intermediary in certain cases- No person providing any service as a network service provider100 shall be liable under this information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Section 84 A – Modes or methods for encryption shall be prescribed by the CG.

Section 84 B –Punishment for abetment of offences- But no express provision made for the length of punishment for abetment to commit an offence under the law.

Section 84 C –Punishment for attempt to commit offences - The section reads 'Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both. The length of punishment is not explicit in the provision and is left to the discretion of the court.

Indian Contract Act, 1872

The *Indian Contract Act*, is two century old law, but complete in all aspects relating to contracts including E-contracts. For a valid contract there are certain requirements to be fulfilled which are, that there should be lawful consideration, the consent should be free, the persons entering into contract must be competent persons (they should not be minor, unsound mind or prohibited under law to enter into contract) and the contract should be made to achieve a lawful object. The Act also deals with the different modes of discharge of contract and also special contracts. Apart from the above requirement, there should be proposal and an unconditional acceptance of the proposal. What one can infer from the above is that the contract enforceable under the law is a process, which has a vital significance in any transaction whether manufacturing or trading or service. The contract has to be valid contract to be enforceable.

E-contract is any kind of contract formed in the course of e-commerce by the interaction of two or more individuals using electronic means, such as email, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract.

In E-Contracts the offer is not made directly to the customer. The consumer 'browses' the available goods and services displayed on

the merchant's website and then choose what he would like to purchase. The offer is not made by website displaying the items for sale at a particular price. This is actually an invitation to offer and hence is revocable at any time up to the time of acceptance. The offer is accepted through e-mails or by just clicking 'I Agree'. The significance of the contract assumes importance in cyber world where anonymity and speed of transaction are key elements. Contracts entered through online process are called as electronic contracts. Electronic contracts helps people to avail the transactions and agreements electronically without meeting each other personally. In an electronic contract normally two parties are involved, the originator and the addressee. The originator is one who sends, stores or transmits electronic messages. The message is transmitted to the 'addressee' is one whom the originator intends to receive the electronic record but does not include intermediary. Intermediary is a person who transmits, stores or receives message on behalf of another or provides any service in respect thereof. If we apply the above theory then in the terms of contract, the result is originator is the promissory; addressee is promise and intermediary is the service of carrier. Electronic message/data can be transmitted without human intervention. As soon as the message is transmitted to the intermediary and is out of control of the originator, it is regarded as delivered.

According to section 12 of the IT Act, if the originator has stipulated for acceptance (I agree) and if that for formalities is completed by the addressee, it becomes a binding/valid contract. The legal requirement of signing the electronic document is also fulfilled by attesting digital signature through a private key assigned to the party by the certifying authority. This part concludes two aspects of contract that is proposal and acceptance. The third part is that the consent must be free that is it must not be taken by coercion, undue influence, fraud, misrepresentation, or by mistake. Among them fraud is both civil wrong as well as criminal wrong. And in commercial transaction, fraud affects the most. In case of banker and customer relationship is a contractual relationship and hence after the advent of E-Banking fraud

has played a pivotal role. Though Indian Contract has defined fraud, but the wrong is civil in nature. The person who has suffered injury or damage can claim only compensation. Fraud committed on banks or by banks is criminal in nature because it involves a deceptive act perpetrated on a victim which is done for personal or financial gain. Hence, the definition of fraud as stated in contract law can be used only to know the meaning and claiming compensation. E-Banking is ultimately an E-Contract and all the provisions of Indian *Contract Act* applies to it *muttasmundadis*.

Indian Penal Code, 1860

Crime is both a social and economic phenomenon. It is as old as human society. In developing economies, cyber crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities. The improvement of online banking system and its increased use by consumers worldwide has made this service a privileged target for cyber criminals. Sweeping amendments were made to certain provisions of Indian Penal Code (herein referred as IPC).Section 172 relating to documents to be produced before a Court of Justice includes electronic records, section 192 on makes false entry in books of records, and section 463, the amendment is inserting false electronic record with the intent to cause damage or injury.

The significant amendment was to section 464 of the Act which is as follows-'A person is said to make a false document or false electronic record, if, first, who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes or *transmits any electronic record or part any electronic record, or affixes any digital signature on any electronic record, or makes any mark denoting the execution of a document or the authenticity of the digital signature,118* with the intention of causing it to be believed that such document or part of a document was made, signed, sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed; or

affixed with, or Secondly.- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or *an electronic record* in any material part thereof, after it has been made or executed or *affixed with digital signature* either by himself or by any other person, whether such person be living or dead at the time of such alteration; or Thirdly.- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or *an electronic record or to affix his digital signature on any electronic record* knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document *or electronic record* or the nature of the alteration. Then section 469, for the words "intending that the document forged" the words "intending that the document or electronic record forged" was substituted. Section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following words were substituted, "Whoever has in this possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or *electronic record* is one of the description mentioned in section 466 of this Code.".IPC is a legislation which is probably the most widely used law in criminal jurisprudence, serving as the main criminal code of India. Offences or crimes have been elaborately dealt under this legislation listing punishment for each offence. IT Act 2000 has amended the sections dealing with records and documents in the IPC by inserting the word 'electronic' thereby treating the electronic records and documents on par with physical records and documents. The sections dealing with false entry in a record or false document are (ex. 192, 204, 378, 383, 463, 464, 468, 469, 470, 471, 474, 476, 499 etc.) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records. Internet frauds in India are recent phenomena but over the

years, it has emerged like an organized crime. Hackers may be anywhere in the world and employ any technique to commit the fraud. Even mobile transactions are hit by the frauds.

There are three crucial elements which are considered responsible for the commission of frauds in banks:

a. Involvement of bank's employee or in connivance with outsiders;

b. Failure of the bank staff to follow the instructions and guidelines; and

c. External elements or collusion between various parties or by a hacker.

Though there are various kinds of frauds, but purely from reporting standpoint, RBI has classified frauds on the basis of the provisions of the IPC

a. Misappropriation (Section 403 IPC) and criminal breach of trust (Section 405 IPC);

b. Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property (Sections 477A, 378 and 120 A);

c. Unauthorized credit facilities extended for reward or for illegal gratification;

d. Negligence and cash shortages;

e. Cheating (Section 415 IPC) and forgery (Section 463 IPC);

f. Forgery of electronic records (Section 465 IPC);

g. Bogus websites, cyber frauds, phishing (Section 420 of IPC)

h. Irregularities in foreign exchange transactions; and

i. Any other type of fraud not coming under the specific heads as above.

Though no specific section defines fraud, all the above provisions are related with the offence. The courts in India have dealt with E-Banking frauds combining sections of IPC and IT Act. Ex. *Syed Asifuddin and Ors. v. The State Of Andhra Pradesh and others*, where case was registered under Sections 409, 420 and 120B of IPC, 1860 and Section 65 of the IT, 2000, the court stated 'whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakhs rupees or both.

Further, while giving explanation to section 65 of the IT Act it stated the word "dishonestly" shall have the meaning assigned to it in section 24 of the IPC and the word "fraudulently" shall have the meaning assigned to it in section 25 of the IPC.

To mitigate this confusion, a definition of fraud was, however, suggested in the context of electronic banking in the Report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, which reads as 'a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.

Indian Evidence Act, 1872

The enactment and adoption of the *Indian Evidence Act* was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian courts of law. The nature of evidence in the real world and virtual world is different. This disparity is conspicuous in all the stages

of evidence detection, gathering, storage and exhibition before the court. Contrary to the real world crimes, where tangible evidences in the form of finger prints, weapon of crimes, blood stain marks, can be traced, in the virtual world such traces becomes very difficult to find. The process of preservation of cybercrime evidences lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to diminutive value of the evidence.

Once the required evidence is identified than the investigator must ensure that the same is collected by adhering to the legal requirements. The legal requirement are, evidence is collected only after the requisite warrant for is issued, if the information appears to be outside the scope of the warrant then additional warrant be issued, completion of the investigation, and other formalities. The evidence collected becomes valid in the court of law only if the evidence is collected by legal means. The *Indian Evidence Act* was amended according to the requirements of the IT Act. The *Indian Evidence Act* gave recognition to all electronic records and documents. In the definition part of the Act, the amendment was made to the word documents which are as follows 'where the word all documents includes electronic records'. Words like 'digital signature', 'electronic form', 'secure electronic record', 'information' as used in the IT Act, were all inserted to make them part of the evidentiary mechanism in the legislation. The under section 17, for the words 'oral or documentary' the words 'oral or documentary or contained in electronic form was substituted. Then section 35 of the Act was amended for the word 'record', in both the places where it occurs, the words 'record or an electronic record' was substituted. Section 39 of the original Act deals with evidence to be given when statement forms part of a conversation, document, book or series of letters or papers.- 'When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or of a connected series of letters or papers, evidence shall be given of so much and no

more of the statement, conversation, document, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made'. The substituted wordings of the section, what evidence to be given when statement forms part of a conversation, document, *electronic record*, book or series of letters or papers- 'When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is *contained in part of electronic record* or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, *electronic record*, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made'. Section 47 was amended and section 47A which emphasis on the opinion as to relevancy of digital signature reads thus- 'when the court has to form an opinion as to the digital signature of any person, the opinion of the certifying authority which has issued the Digital Signature Certificate is a relevant fact'. Section 59 was also amended where the word 'contents of documents', were substituted with words 'contents of documents or electronic records'. Section 65 was amended and two subsection section 65A and 65B were inserted. 65 A deals with special provisions as to evidence relating to electronic record and 65B deals with admissibility of electronic records. The other amendments were relating to proof as to digital signature, proof as to verification of digital signature, presumption as to electronic records and digital signatures, presumption as to digital signature certificate, and production of documents or electronic records which another person, having possession, court refuses to produce before courts. Amendments brought to *Indian Evidence Act* were questioned in *P. Padmanabh v. Syndicate Bank Limited*, where court held admissibility of electronic records, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred as the

computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Admissibility of electronic records as evidence as enshrined in section 65Bof the *Indian Evidence Act* is wide enough to cover all types of electronic records as evidence which states as under-

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data.

And thus ensuring integrity of data produced directly with or without human intervention accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the section.

Consumer Protection Act, 1986

Consumer protection in India got a boost with the enactment of *Consumer Protection Act, 1986.* It provided a power in the hands of

> *'Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied: (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly.... by lawful persons.. (b) the information ...derived was regularly fed into the computer in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer was operating properly r was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities'*

Indian consumers to get appropriate, timely and effective grievances redressal against companies and individuals who had provided defective good or deficient services. It has been most effective weapon in the hands of consumers for claiming compensation through speedy redressal. Speedy justice which is fundamental right of the citizens of India has been guaranteed is ensured in this Act. It is a board which is constituted and many of the formalities which are required to be followed in the normal courts need not followed. The justice is ensured by a bench headed by a chairman and two social workers who sit and listen to the matter. Both documentary and oral evidence are taken. Material objects are also examined and justice is ensured. Customer of a bank is also a consumer as he fits into the definition of consumer under the law. Consumer is a person who buys or hires and goods or services for a consideration, i.e. free services are not covered under the Act.

It excludes a person who buys or hires for commercial purpose/activity and not for self-consumption. The National Consumer Forum has held that once it is found that there is hiring of service for consideration and that loss has been caused to the complainant on account of negligence and deficiency in rendering the service, the aggrieved consumer is entitled to seek remedy under *Consumer Protection Act* and the aggrieved consumer is also entitled to seek redressal from appropriate forum. Technological failure and providing confidential details have been treated as deficiency of service in banks provided the customer has not acted negligently. The bank should give instruction to the customer before providing them with E-Banking facility. Internet banking has now started motivating customers to park their funds with the online banks, which has a substantially impact on the deposit base of the brick and mortar banks. And the same should be encouraged with precautions.

The Payment and Settlement Systems Act, 2007

It is internationally acknowledged that payment and settlement systems should function on a well-founded legal basis. This entails

among other things, proper authorization requirement for setting up and payment systems, legal recognition for netting, settlement finality, providing for regulation and oversight of the payment and settlement systems. In India there is no enactment which dealt with the issue of Electronic Fund Transfer (EFT). *The Payment and Settlement Act* (herein referred as PSS Act) and the directions and guidelines issued there under deal, to a certain extent, with the issue. In order to strengthen the institutional framework for the payment and settlement systems in the country, the RBI constituted, in 2005, a Board for Regulation and Supervision of Payment and Settlement Systems as a Committee of its Central Board. The Board which was chaired by the Governor of RBI, while all the four Deputy Governors and two external Directors of the Central Board are its members. Based on the recommendation of the board the present legislation i.e. *The Payment and Settlement Systems Act, 2007* was drafted which gave wide powers to RBI to govern the payment system in the country. Object of this legislation is to establish safe, secure, sound and efficient payment and settlement systems for the country. Whereas safety in payment and settlement systems relates to risk reduction measures, security pertains to confidence in the integrity of the payment systems. All payment systems are envisaged to be on sound footing with adequate legal backing for operational procedures and transparency norms. Efficiency enhancements are envisaged by leveraging the benefits of technology for cost-effective solutions. "Payment Instruction" is defined 'as any instrument, authorization or order in any form, including by electronic means, to effect a payment by a person to a participant in a payment system or from one participant in such a system to another participant in that system. The payment instruction can be communicated either manually i.e. through an instrument like a cheque, draft, payment order or through electronic means, so that a payment can be made by either a person to the participant in such a system or between two participants'. Payment system" includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. The RBI has considered factors like, the need for the proposed payment system, the technical

standards and design of proposed system, the security procedures and terms and conditions of operation of the proposed system, the procedure for netting of payment instructions, risk management processes, financial status of the applicant, experience of management and integrity of applicant, consumer interests, monetary and credit policies and other relevant factors while authorizing any institution who apply for payment through electronic means. RBI has laid down conditions to be fulfilled by the institution to obtain the authorization letter. The Act lays down an elaborate mechanism for settlement of disputes between system participants in a payment system, between system participant and system provider and between system providers. The RBI is empowered to call for from the system provider returns, documents and other information relating to the operation of the payment system. The system provider and all system participants are required to provide Reserve Bank access to any information relating to the operation of the payment system. Under this legislation, dishonour of an electronic fund transfer instruction due to insufficiency of funds in the account is an offence punishable with imprisonment or with fine or both, similar to the dishonour of a cheque under the NI Act, 1881. Subject to complying with the procedures laid down under the Act, criminal prosecution of defaulter can be initiated in such cases. Hence under this legislation the RBI is able to monitor the electronic payment system in India

CONCLUSION

Internet banking and mobile banking have transformed not only the banking relationships but transformed the whole banking industry. Through Internet and Mobile banking, customers can process any banking transaction without even visiting bank at anytime, anywhere and this is known as anywhere Banking.

National Cyber Security Policy -2013

Preamble

1. Cyberspace1 is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc.) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms

and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism,

cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

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

III. Objectives

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical

Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment

of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.

6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.

5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

INFORMATION SECURITY BEST PRACTICES

MINISTRY OF HOME AFFAIRS

1. Introduction

Ministry of Home Affairs, Cyber & Information Security (CIS) Division has prepared this document to disseminate Information Security best practices for the benefit of Government Officials/Officers. This should not be considered as an exhaustive list of prescription for Information Security but basic minimum precautions to be taken. Each organization should identify additional measures for information security in accordance with their use scenarios, sensitivity of data, business continuity and other relevant factors.

2. General Computer Usage

Following are some of the best practices for computer use on day to day basis:

2.1 All classified work should be strictly carried out only in a standalone computer which is not connected to the internet.

2.2 Create strong passwords for login by using a combination of letters, numbers, and special characters with minimum of 10 characters.

2.3 Computers should be protected from virus/worms using an Antivirus software permitted for use by your organization.

2.4 Make sure your operating system, application and software patches including anti-virus software are up to date; and auto updates are turned on in your computer.

2.5 Don't leave the computer unattended with sensitive information on the screen.

2.6 Always lock your computer before leaving workplace to prevent unauthorized access. A user can lock computer by pressing„ctrl +alt+del‟ and choosing „lock this computer‟ or “window button+ L”.

2.7 Enable a password-protected screen saver with a timeout period of 2 minutes to ensure that computers that were left unsecured will be protected.

2.8 Be careful of what you plug in to your computer. Malware can spread through infected USB drives, external hard drives, and even smart phones.

2.9 Use non-administrator account privileges for login to the computer and avoid accessing with administrator privileges for day-to-day usage.

2.10 Treat sensitive data very carefully and use encryption to securely encode sensitive information.

2.11 Backup your important files at regular intervals to avoid unexpected loss.

2.12 Remove unnecessary programs or services from computer which are not required for day to day operation.

2.13 Do not give remote access, file and print sharing option to other computers.

2.14 Do not use file sharing softwares as file sharing opens your computer to the risk of malicious files and attacks.

2.15 Avoid entering sensitive information onto a public computer like cyber cafe, library computers etc.,

2.16 If you store or download any personal information on computers in cyber café, make sure you delete permanently all the documents after you are done with your work. You may press Shift and Delete button together to make it difficult to recover deleted files.

2.17 Remove files or data you no longer need to prevent unauthorized access to such data. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system. File shredder software should be used to delete sensitive files on computers.

2.18 Ensure to use un-interrupted power supply to computers through UPS or other backup sources.

2.19 Do not plug the computer directly to the wall outlet as power surges may damage computer. Instead use a genuine surge protector to plug a computer.

2.20 The systems should be placed in a room which is dust free and has a good ventilation to avoid overheating of CPU.

3. General Internet Browsing

Following are some of the best practices to keep in mind when browsing on Internet:

3.1. Always be careful when clicking on links or downloading. If it‟s unexpected or suspicious for any reason, don‟t click on it.

3.2. Do not download any type of files/software from any source other than those allowed by your system administrator/department.

3.3. Use web browser which has been permitted by your Organization.

3.4. Always use updated web browser for browsing. If you run a web browser that is out of date, it may contain security vulnerabilities and you risk having your computer compromised. Depending on the security exploit, your personal information (including emails, banking details, online transactions, photos and other sensitive information) could be stolen or destroyed.

3.5. Do not store/ share any sensitive information on any device that is connected to the Internet.

3.6. The "Save password" option prompted by the browser should not be selected if a window appears after entering information on the login screen, asking you to do so. Don’t save account

information, such as passwords or credit card information in web browsers, especially on those PCs which are shared with other users.

3.7. Look for HTTPS sign in the browser address bar. The “s” in “https” stands for secure, meaning that the website is employing SSL encryption. Check for an “https:” with a green padlock icon in your browser address bar to verify that a site is secure.

3.8. Make a habit of clearing history from the browser after each logout session. Following are the settings in various browsers to automatically clear the history on each browser session ends:

Chrome

- Click on the menu icon in the upper right corner and select Settings> Show advanced settings... >Privacy and then tap the Content settings button.
- In the next window that opens, under Cookies, enable the option that says "Keep local data only until you quit your browser."
- Press Done at the bottom of the window.

Firefox

- Click on the menu icon in the upper right corner and select Options. Then in the window that opens, click on the Privacy tab.
- Under History, click the drop down menu next to "Firefox will:" and select Use custom settings for history.
- Check the option Clear History when Firefox closes.
- Once you're done click OK.

Internet Explorer

- Click settings icon in the upper-right corner of the browser and select Internet Options.
- Open the General Tab in the window that appears.

- Under the Browsing History section, check the box next to "Delete browser history on exit." Once you're done click OK.

3.9. No classified information of government can be stored on private cloud services (Google drive, Dropbox, iCloud etc.,) and doing so may make you liable for penal action, in case of data leakage.

3.10. When on tour, avoid using services that require location information, unless it is necessary for discharge of office duties.

3.11. While browsing, some pop-ups may appear with option of close button.These may be fake and may actually try to install spyware when you click on it. Beware of such pop-ups and avoid clicking on it.

3.12. Popup blocker option should be kept turned ON in the browser and may be selectively allowed for trusted sites, if required. Doing so will help prevents any nuisance web ads or malware embedded in ads from appearing on screen. Following are the setting to turn on popup blocker configure in various browsers:

Firefox

- Select Tools from the Mozilla Firefox taskbar
- Select Options from the drop-down menu
- Select Content from the Options dialog box
- To enable all pop-ups, check the Block pop-up windows radio button
- Click Close

Chrome

- Click on the Menu
- Click on Settings
- Scroll to Privacy, Click on Content Settings
- Scroll to Pop-Ups
- Uncheck Allow All Sites to show Pop-Ups
- Click OK

Internet Explorer

- Click Tools menu
- Click Internet Options
- Click Privacy tab
- Under Pop-up Blocker, Check Turn on Pop-up Blocker
- Click OK

3.13. Remember that things on the internet are rarely free. "Free" Screensavers etc., often contain malware.So be aware of such online free offers.

3.14. Avoid using public computers and public Wi-Fi connections to access and carryout any financial or sensitive transactions. Accessing government email on such computers has a risk of causing information breach.

3.15. If your job requires you to access certain information systems in a secure way, it is advisable to use security controls such as MPLS link, VPN over internet etc., for such access.

4. Password Management

Unauthorized access is a major problem for anyone who uses a computer or devices such as smartphones or tablets. The consequences for victims of these break-ins can include the loss of valuable data such as classified information, personal data etc. One of the most common ways that hackers break into computers is by guessing passwords. Simple and commonly used passwords enable intruders to easily gain access and control a computing device. Following are some of the best practices to consider while setting up and managing a password,

4.1. Create strong password with a minimum length of ideally 10 characters and comprising of mix of alphabets, numbers and characters.

4.2. All passwords (e.g., email, computer, etc.) should be changed periodically at least once every three months.

4.3. Don't reuse old passwords.

4.4. Passwords should not be stored in readable form in computers, notebook, notice board or in any other location where unauthorized persons might discover or use them.

4.5. Treat passwords as sensitive information and do not share it with anyone.

4.6. Always use different passwords for every log-in accounts you have. Using the same password for more than one account risks multiple exposures if one site you use is hacked.

4.7. If your work requires you to communicate passwords, such as while sending password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS.

4.8. Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.

4.9. Remember weak passwords have the following characteristics:

- The password contains less than 10 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, colleagues, Movie / Novel / Comics characters, etc. Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.

- Word or number patterns like 123456, aaaaa, qwerty, asdfg, zxcvb, etc.

4.10. Some suggested way to construct a strong password are as follows,

- A secure password not only consist of letters, must also use numbers, special characters and caps. One suggested way to replace letters with numbers and special characters, so an "i" will become "!", an "o" turns into a "0" and "s" is written as "$". This way, the simple term "Microsoft" changes to the substantially harder word "M!cr0$0ft".
- Password length matters, the longer the password, the harder it is to crack.
- Think of a sentence and select the first letters of each word in a row will get a complex password and easy to remember as well.

For example, sentence like this, "My Name is Dinesh Anandan and I was born on 1 January 1986!" would produce the following password: "MNiDAaIwbo1J1986!". It "slong, contains numbers, special characters, caps and letters, and it's easy to remember and won't be in dictionary.

5. Removable Information Storage Media

One of today's biggest security concern is the use of removable storage devices (USB devices such as pen drives, CD-RW, DVD-RW, Blu-ray discs, Media cards etc.,) in their networks. The amount of data that can be quickly copied to removable storage devices is increasing every day. While these devices can significantly boost productivity, they can also cause dangerously high risks in data security and control policies. External removable portable storage devices allow users to bypass perimeter defenses, including firewalls and email server anti-malware, and potentially introduce malware into the office network. Since the malware enters the network from an internal device, it may go undetected until significant damage is caused

to the network. Removable storage devices also facilitate easy pilferage of sensitive information from an organization's premises. This information might include classified information. Following are some of the best practices to be considered while dealing with Removable storage media:

5.1. Auto run/ Auto play feature must be disabled for all removable media.

5.2. The classified data should be encrypted before copying into the removable storage media designated to store classified information.

5.3. Classified information should be stored only on organization allocated removable storage media for work purpose.

5.4. The computers should be enabled with “Show hidden file and folders” option to view hidden malicious files in USB storage devices.

Steps to enable hidden file & system file view to find any unusual or hidden files in computer are as follows:

Windows 10

- In the search box on the taskbar, type folder, and then select Show hidden files and folders from the search results.
- Under Advanced settings, select Show hidden files, folders, and drives, and then select OK.

Windows 8.1

- Go to Search.
- Then type folder in the search box, then select Folder Options from the search results.
- Select the View tab.
- Under Advanced settings, select Show hidden files, folders, and drives, and then select OK.

Windows 7

- Select the Start button, then select Control Panel -> Appearance and Personalization.
- Select Folder Options, then select the View tab.

5.5. It is advisable to scan all removable media with anti-virus software before use.

5.6. Removable media like USB‟s, CDs etc., must not be left unattended.

5.7. Technical controls may be implemented to restrict use of portable storage media drives outside of the Government network.

5.8. Removable media should not be taken out of office unless permitted by the competent authority in your office.

5.9. In order to minimize physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

5.10. In case of damage or malfunction of device, the same should be returned to the designated authority in your office for repair/replacement. Never ever handover such devices to outsiders or other vendors for repair as it might have classified information.

5.11. If the USB device is no longer a functional requirement after issuance, then the same should be returned to the issuing authority.

5.12. The contents of removable media must be removed/erased after the official purpose has been served.

6. Email Communication

Following are some of the best practices in regards to email communication:

6.1. Use only Government provided email address for official communications (e.g. nicemail).

6.2. System administrator may deploy appropriate controls to restrict use of personal email address for any official communications.

6.3. Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.

6.4. Classified information be not communicated via emails. In case of emergent requirements to do so, the approval of competent authority should be obtained.

6.5. Avoid accessing official email accounts from public Wi-Fi connections.

6.6. Auto save of password for email accounts should not be enabled.

6.7. Logout from mail accounts after your work is done.

6.8. User should type the complete URL in the browser instead of clicking links received in an email.

6.9. Do not open / forward / reply to any suspicious e-mails.

6.10. Be cautious on tiny or shortened URL‟s (appears like http://tiny.cc/ba1j5y) and don't click on it as it may take you to a malware infected website.

6.11. Do not open attachment having extension such as EXE, DLL, VBS, SHS, PIF, SCR. Typical example., .txt.exe, .doc.exe

7. Home Wi-Fi Network

With the mass explosion of Laptops, Smart Phones and Tablets, pervasive wireless connectivity is widely used an option for connecting to the Internet. Insecure wireless configuration can provide an easy open door for malicious threat actors. Government officials may use their home Wi-Fi network to do office work and in order to

secure their home Wi-Fi network, following are some of the best practices:

7.1. Turn on WPA2 or higher encryption feature in wireless routers.

7.2. Change the default network device name, also known as its service set identifier or "SSID." When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. It is advisable to have SSID name which does not disclose your identity in any manner.

7.3. Change the network device default password. Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password.

7.4. Consider using the Media Access Control, or "MAC," address filter in your wireless router. Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept connections only from devices with MAC addresses that the router will recognize. To create another obstacle to unauthorized access, consider activating your wireless router's MAC address filter to include your devices only.

7.5. Turn off your wireless router when not needed for any extended period of time.

7.6. Update the firmware of wireless devices regularly as it will reduce the number of security loop holes in the device.

7.7. Disable remote management feature in routers to protect against unauthorized access.

8. Use of Social Media by Government Officers/Officials:

All personnel including employees, contractual staff, consultants, partners, third party staff etc., who manage, operate or support information systems, facilities, communication networks; and information created, accessed, stored and processed by or on behalf of the Government of India, unless authorized to do so, shall not:

a. Access social media on any official device (computer, mobile etc.).

b. Disclose official information on social media or social networking portals or applications.

9. Avoiding Social Engineering Attacks

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email. Following are some of the best practices should follow to avoid social engineering attacks:

8.1. Be careful to unsolicited phone calls, visits, or email messages from individuals asking about personal or other Government information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

8.2. Phishing is one of common type of social engineering scam. The hacker typically sends an email or text to the target, seeking information that might help with a more significant crime. So do not reveal personal, sensitive or financial information in email or messages, and do not respond to such emails.

For example, a hacker might send emails that appear to come from a source trusted by the victim. That source might be a bank for instance, asking email recipients to click on a link to log in to their accounts. Those who click on the link, though, are taken to a fake

website that, like the email, appears to be legitimate. If they log in at that fake site, they‟re essentially handing over their login credentials and giving the crook access to their bank accounts.

8.3. Vishing is the voice version of phishing. “V” stands for voice, but otherwise, the scam attempt is the same. The hacker uses the phone to trick a victim into handing over valuable information. So don‟t reveal any sensitive information over phone calls.

For example, a hacker might call an officer, posing as a Government officer. The hacker might prevail upon the victim to provide login credentials or other information that could be used to target the Organization.

8.4. Quid pro quo scam is another type of social engineering attack that involves an exchange like I give you this, and you give me that. Hackers make the victim believe as a fair exchange, but that‟s far from the case, as the cheat always comes out on top.

For example, a hacker may call a target, pretending to be an IT support technician. The victim might hand over the login credentials to their computer, thinking they‟re receiving technical support in return. Instead, the hacker can now take control of the victim‟s computer, loading it with malware or, perhaps, stealing personal information from the computer to commit identity theft.

8.5. Be cautious of the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). In general, all government websites have gov.in or nic.in at the end of their names. For example, a malicious website may have name as www.npagov.in or www.npa-gov.in against the actual name www.npa.gov.in

8.6. It‟s safer to type a URL into your browser instead of clicking on a link. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

8.7. Hacker wants you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let the urgency influence your careful review.

8.8. If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam and do not respond and delete such emails.

8.9. Immediately change any passwords you might have revealed to anyone. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

10. Glossary

Term	Definition
DDoS	A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
Digital Signature	A digital signature is a way to ensure that an electronic document (e-mail, spread sheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any

	way since that person created it.
DNS	The domain name system (DNS) is the way internet domain names are located and translated into internet protocol addresses.
Encryption	Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.
GPS	The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information.
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer is a URL scheme used to indicate a secure HTTP connection.
IM	Instant Messaging a type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet.
IoT	Internet of Things (IoT) is an ecosystem of connected objects that are accessible through the internet.
Malware	Malware is short for malicious software and used as a single term to refer to virus, spy ware, worm etc.
SMS	SMS is a text messaging service component of most telephone, internet, and mobile-device systems.
SNMP	Simple Network Management Protocol is used in network management systems to monitor network attached devices for conditions that warrant administrative attention.

SSH	Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two computers.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LAN to which a client wants to attach.
Trojan	A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.
URL	A Uniform Resource Locator (URL), colloquially termed a web address is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
USB	A Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer.
Virus	Virus is a program written to enter to your computer and damage/alter your files/data and replicate themselves.
VPN	A virtual private network extends a private network across a public network, and enables users to send and receive data across shared

	or public networks as if their computing devices were directly connected to the private network.
Wi-Fi Certified	Wi-Fi certified is a program for testing products to the 802.11 industry standards for interoperability, security, easy installation, and reliability.
Worms	Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc.

NOTE:

- In case of any doubt, *National Information Security Policy & Guidelines* (NISPG) issued by Ministry of Home Affairs may be referred to.
- Due care has been taken while preparing this booklet. If any suggestion for improvement(s) is felt, same may be shared at cyberdost@mha.gov.in.