Journal of Social Welfare and Management
Volume 10 Number 2, May - August 2018

Need of Cyber Security in Digital India

M.L. Himaja

Abstract

Information technology is the architect of the present world. It has given a new structure of the world as well as to society. For any transmission that may be information or an idea or goods or few of services or money everything can be done in the cyber space. This is more encouraging to conduct a cyber crime with reference to corresponding operation by the criminals. Once any one landed on this platform to perform they are not only connected to the world, and also welcoming a huge number of known and unknown people in to their personal world too. At this point of time cyber security take a lead to drive the process and safeguarding like a shield for individual data base in the cyber space. It also defends from unnecessary accessibility of one's information by the others and controls the cyber crime.

At present most of the financial transactions happened through online due to reasons like ease of transaction facility, government policy and to avoid physical cash payment. So everyone have just around the corner of their information by others. In the view of this, protecting the financial information of individual or organizations is a gigantic challenge in front of the information technology industry. The present paper is analyzing how threats takes place in the online transaction process and what are the recommendations to be practiced against those threats by providing more reliable security though cyber security methods and information technology techniques.

Keywords: Information Technology; Cyber Space; Cyber Crime; Financial Transactions.

Introduction

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

The present techno-sense environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. With a span it will turn into more transactional with e-business, e-commerce, e-governance and e-procurement etc. and also it creates a base for certain illegal practices by criminals known as cyber criminals. Here all legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great forward motion. Because of the digitalization almost all everything related to cyberspace, where we can find cybercrime too, cyber security and cyber law implications are most optimal to lever the situation.

Literature Review

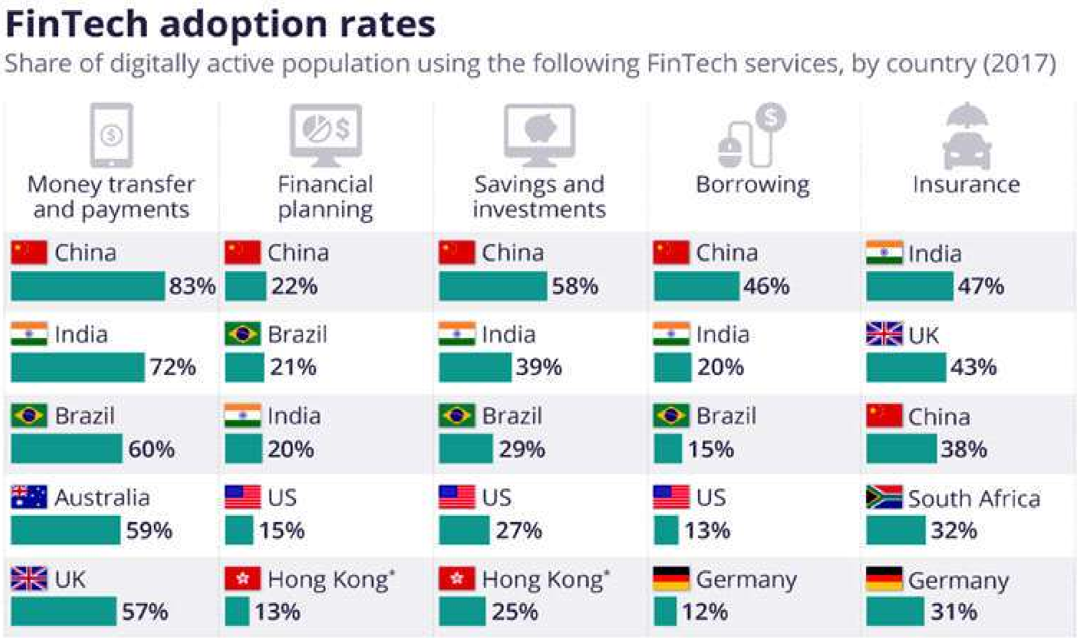
Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes

Author's Affiliation: Assistant Professor, Department of MBA, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana State, India - 500100.

Reprint's Request: M.L. Himaja, Assistant Professor, Department of Business Management, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana State, India - 500100.
E-mail: himajamba2005@gmail.com

Received on 13.06.2018, **Accepted on** 20.06.2018

Table 1: Usage of information technology for financial operations



FinTech adoption rates

Share of digitally active population using the following FinTech services, by country (2017)

Money transfer and payments	Financial planning	Savings and investments	Borrowing	Insurance
China 83%	China 22%	China 58%	China 46%	India 47%
India 72%	Brazil 21%	India 39%	India 20%	UK 43%
Brazil 60%	India 20%	Brazil 29%	Brazil 15%	China 38%
Australia 59%	US 15%	US 27%	US 13%	South Africa 32%
UK 57%	Hong Kong* 13%	Hong Kong* 25%	Germany 12%	Germany 31%

*Hong kong is special administrative region of the Peoples' Republic of China

like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on.

Digital environment in India is wide spreading. Be it financial or non-financial in nature. One can observes the usages of digital media in following transactions.

- Most of transactions in shares are in De-mat form.
- Companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit/debit cards for shopping.
- Most people are using email, phones and SMS messages for communication.
- Even in "non-cyber crime" cases, important evidence will be the electronic gadget which has the capacity to store the information eg: in cases of murder, divorce, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.

Table 2: Cyber Law of India

Time	Event
October 2000	Information Technology Act 2000 came into force.
2006	Cyber Appellate Tribunal (CAT) started functioning
2008	NASSCOM established the DSCI.
December 2008	Information Technology (Amendment) Bill 2008 passed by Indian Parliament
February 2009	The IT (Amendment) Act 2008 received the assent of the President
October 2009	The IT (Amendment) Act 2008 came into force
2011. October	The central bank, RBI introduced a set of recommendations, which include the formation of separate information security groups within banks and maintenance of adequate cyber security resources based on their size and scope of operation
October 2012	Cyber security joint working group (JWG) released its "Engagement with Private Sector on Cyber Security" report.
July 2013	The government released the NCSP, which set forth 14 objectives that included enhancing the protection of critical infrastructure and developing 500,000 skilled cyber security professionals in the next five years
April 2017.	The IRDAI issued guideline, which require all insurance companies to appoint a CISO

Source: National Crime Records Bureau (NCRB)

Research Objective

1. Understand the digital environment in India.
2. Interpret the transactional process and cybercrimes and laws.
3. End with certain recommendations

Research Methodology

Secondary data analysis.

Data Analysis and Interpretation

Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common in financial services(With reference to Table 1).

Digital signatures and e-contracts are fast replacing conventional method of transacting business.

With the sense of all we can understand that cyber security is that cyber attacks are not only restricted to the financial services and banking sector. It is important to note that industrial companies are equally vulnerable. At the same time, it has become clear that predictable IT systems and firewalls are increasingly becoming ineffective in preventing complicated hackers from creating confusion for this first we should understand the concept of cyber security

Crimes can be classified broadly in to two

1. Known
2. Unknown

In the same way reasons for cybercrime also be categories into three types

- Lake of awareness about cyber attacks
- Poor security arrangement
- Rapid technological development from criminal end

From the information, most of the attacks realizes only after once the loss takes place in the organization even though we are good enough to use the technology but not completely exposed to safeguarding our information as well as identifying threats this may leads to have cyber attack turn into huge loss. Here we can to identify a gap because of inaccurate communication about the crime to host that is service provider of internet. It happens due to service providers are different from users. Even though by providing different kind security protocols like OTP, Pass words and authenticated accessibility we are welcoming the risk in to our path.

The criminal activities are one step forward to the technical procedure followed by the service providers and therefore, are able to breach the security.

Components of Cyber Security

Let us see different components in the cyber security space

- Data security
- Software security
- System security
- Human security
- Organizational security
- Societal security

While most of these components are technical, factors like human and societal security also have lasting repercussions on a company's digital security. Accidental disclosure of information is a common issue threatening the leakage of confidential company data. This may happened because of mobility of the devices and flexibility in working place. These two situations demand the user to access the unstructured connectivity which was nearly available to access the internet So be careful the next time you are cheerfully talking about an eventful day at work on social media – your business competitors may be keeping a close watch on it.

In the past the attacks have been initiated from forward countries like US ,UAE, China but extensive use of internet and smart phones in India became a primary target for cyber criminals.

Year by year cyber attacks in India rising.

According to a report by *Hindu Business Line*, 15 crore of the total 230 crore e-transactions that took place last week were compromised. Given the government's Digital India policy which involves registering over a billion people on a unique ID, Aadhaar, and the subsequent controversy over user privacy, these findings are worrisome.

The report quotes sources highlighting that 40 percent of cyber attacks in India today impact financial and government websites. The most common of these attacks involve *Phishing, DoS, and Ransom ware attacks.*

According to an official quoted in the report, most of the breaches occur on Gmail accounts, and could be attributed to the fact that 'the maximum number of internet users (500 million) have smart phones based on Android' The cost of cyber attacks in India currently stands in excess of Rs25,000 core ($4billion). It is important to note that there are many cyber attacks that go undetected and unreported as well, so this number could be much higher.

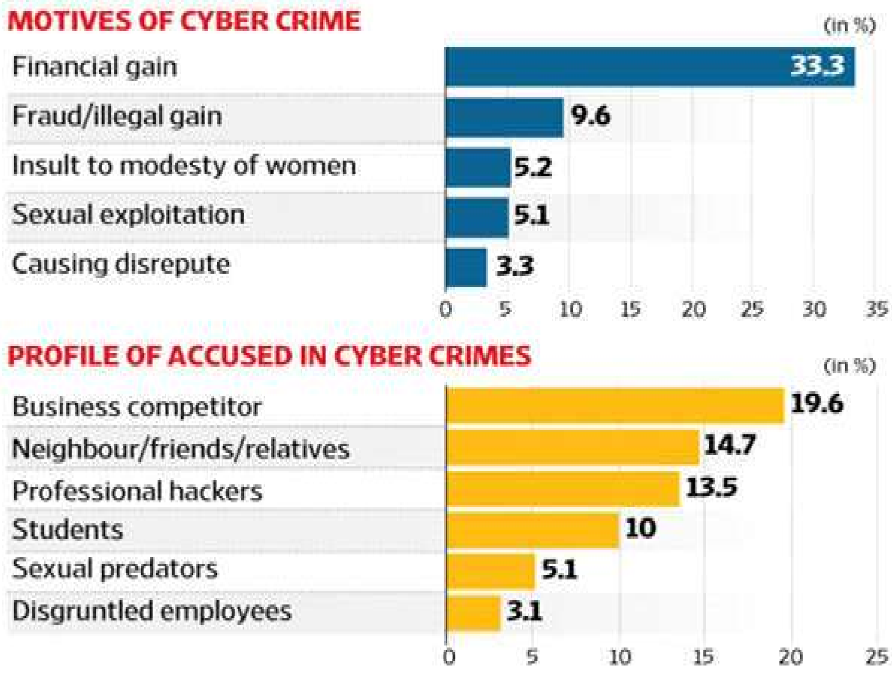
This losses originate commencing operational disruptions, loss of sensitive information and designs, customer agitate and impact on brand image, as well as increase in legal claims and insurance premium. The issue is forecast to balloon further in the coming years, reaching as high as Rs1.25 trillion ($20 billion) over the next 10 years, as the business operations of most Indian companies become networked.

Findings

Many companies do not care for it as a strategic agenda, but rather as a small issue for their IT departments. In fact, a lot of cyber security incidents go undisclosed and hence, unreported.

From the table 3can understand that most of the accused ones belongs to corporate or business persons and the motive is either financial gain or financial loss. To control the cyber crime we need for specialized and customized industry-specific cyber security measures which are significantly different from IT security and need to be adapted by the industry. This will help you to understand complete picture of cyber space which include require skills sets to operate, different types of attacks and safety measures

Table 3: Information about reason for cyber crimes and different set of accused



Source: NCRB report (2016)

With this stand we needed to consider the below things to provide optimal security

Asset identification and valuation

- Threat assessment
- Vulnerability analysis, and
- Safeguarding/Counter-measuring selection

Once the risk is analyzed, the next step is to deep dive into the vulnerabilities, which include:

Find vulnerabilities - Look for weaknesses in servers, Operating System and software.

Highlight flaws – Ensure that systems are updated, look into patch management of malware and other systems with a threat to malware.

Find security weaknesses in existing and planned systems – Take into consideration aspects like testing existing systems for susceptibility and cost-effectiveness.

Along with the above process we should practice the following also

- Use anti-virus software
- If in doubt, block
- More than one e-mail accounts
- Ignore pop-ups
- Macs are as vulnerable as PCs
- Two-step verification
- Only shop online on secure sites
- Don't attract to words anything with excitement
- Different site, different passwords
- Don't store your card details on websites
- Lock down your FB account
- Don't store your card details on websites

Conclusion

From all the above analysis we can conclude that the major motive of the cyber crime in most of the times is either financial gain or creating financial loss to accused person irrespective of which group they may belongs to and worth. To control the cyber crime society must be Initiating to adopt few rules and regulations to deal with their digital operations

- People must be educated and being with literacy in technical things before start digital operation rather than their sightless usage.
- People should more alert regarding any attack
- Reaction against the attack is mandatory
- correspond immediately to concern departments for recovery
- Service provider and user both should feel more responsibility and accountability for every transaction in cyber space.
- Include the cyber security in strategic agenda
- Insure your data with the cyber insurance companies to minimize/avoid risk
- Social ethics must be observe by the people while they are benefit of huge information in cyber space

References

1. http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article 8327987.ece.
2. http://articles.economictimes.indiatimes.com/2014-01-20/news/46374805_1_cyber-security-web-hosting-attack-surface.
3. Nir Kshetri October 2016, Volume 66, Issue 3, pp313–338 | Universityof Pennsylvania Law Review.
4. Alawadhi, N. Cyber security policy must be practical: Experts. 2014. http://articles. economictimes. indiatimes.com/2014-10.