pISSN: 2454-7107, eISSN: 2455-4189

Indian Journal of Law and Human Behavior
Volume 5 Number 2 (Special Issue), May - August 2019
DOI: http://dx.doi.org/10.21088/ijlhb.2454.7107.5219.16

Original Article

Cyber-Crime: An Unleashed Danger for Developing Countries

Himanshu Mishra

Author Affiliation

2nd year BBA LLB (Hons.), ICFAI University, Dehradun, Uttarakhand 248197, India.

Corresponding Author

Himanshu Mishra, 2nd year BBA LLB (Hons.), ICFAI University, Dehradun, Uttarakhand 248197, India.

E-mail: mishrahimanshu325@ymail.com

Abstract

In the recent years we have seen a reasonably high rate of technology advancement which helped in making some works quite easy and accessible for all of us. But at the same time when these things served boon for us but at the same time it also involved high risks about which most the people were unaware. Most of the electronic equipments are hackable and can be used to gain access to each and everyone's all kind of information which is present on their device and not only this way, there are various other ways which can lead to harm people. And this wasn't just happening in India, it was happening all over the world. All the illegal activities in which electronics (mostly computers) were used came under cybercrime. And the stats clearly shows that the number of cybercrimes are increasing day by day. And it is harder to control in the developing countries as compared to the developed countries, still there are some countries which certainly don't have any legislation against the cybercrime. In this paper we will discuss why the developing countries a bigger prey for the cybercrime rather than developed countries, and what are the further steps or laws can be made so that cybercrime can be prevented to a larger extent.

Keywords: Cybercrime; Legislation; Developed countries.

How to cite this article:

Himanshu Mishra. Cyber-Crime: An Unleashed Danger for Developing Countries. Indian J Law Hum Behav. 2019;5(2):215–220.

Introduction

The decades have been passed from the time when the whole information has to printed and kept as records which need to updated from time to time or for searching a information about a topic people needed to go through hundreds of pages. Now the time has changed, and it will not be wrong to say that drastic evolution take place in the field of electronics and connectivity. All the information was readily available and there was no need to keep searching for it. Though when the evolution was taking part in the field of electronics and people came to know that data can easily be stored in the physical drive (hard discs, SSD etc.) or in virtual drive (like clouds), a lot of data was stored in these drive for easy accessibility and they were secured by using various encryptions to secure them but was the data really secure? And how secure is the thing that keeps us connected?

History of Internet

Internet is the thing that keeps us connects and helps to retrieve the information about anything and from anywhere. Actually Internet is a protocol which is used for addressing device locations and their connections over public communications line and is also the number one threat to the personal privacy humankind has ever faced. It facilitates communication and the exchange of information in a way that puts that information, the connections over which it is communicated and the parties involved at risk of theft, damage and worse. When you enter it, connect to it, you send ripples across it that alert others to your presence. Because the net is part of the public domain anyone can use it, for any purpose they wish, and in all too many cases this means no good. To fully understand the threats of internet we need to understand that internet is not a physical thing though it includes our computers, devices, servers routers and other network structures. Before the Internet there were computer networks run by the government, the military, private corporations and any other organization with the resources to run one. To access one of those early networks you had to either be logged into a device on the network or gain access remotely through a modem. In those days this wasn't like it is today where you just enter a web address in your browser and get taken there automatically. No, in those days users would have to dial each network directly from their phone, wait for the confirming squeal of the connection, and then access it slowly. And if they wanted to go to a different network the process would have to be repeated each time. The TCP/IP solved problems faced by early computer network users. It provided the means by which computers could identify each other and how to find each other. This is done through IP (Internet Protocol) addresses, one of which is assigned to each and every device on the web. In order to find other devices the IP addresses have to be visible for others to see which raises one of the very first privacy issues: how can you stay private if everyone can see who and where you are? Because this was such a big issue lots of people were working on it. At heart there were two issues. The first is that IP addresses are visible which makes connections visible, traceable and hack-able. The second is that the data itself was at risk, even if connections could be secured there is still a risk of loss. The final solution is a combination of fixes from private sector and government sources called virtual private network. Virtual private network, VPN, is a means of securing Internet connections when using a public network that solves both issues. The first, visibility, was solved with the Tunneling Protocol. This protocol is a means of forming connections that mask IP addresses and bypasses local ISP servers in favor of dedicated VPN servers. The VPN servers were run by whichever local network operator had the resources to set one up. The second problem, data integrity, was solved with encryption. All data that is transmitted across enabled VPN networks is encrypted so that if intercepted, it won't be usable. The average Internet user did not have access to VPN in the early days of the web. This left them open to many forms of fraud and sparked the industry that we know today as Internet Security[1].

Relation of Cyber Crime with Law

In the early years when the computers were not readily available than also there were cases of computer crime as the study suggests that the first stage of computer crime lasted through the late 1960s. Even when there were cases related to computer crime, the legislature did not provide any specific countermeasures against the phenomenon, leaving the law enforcement to deal with it within the traditional legal framework. With the emergence of the cyber-criminal phenomenon, the principle of "nullum crimen, nulla poena sine lege" was applied to protect the fundamental rights of the perpetrators from punishment outside the law. Except for the reluctant application of old laws, there was neither a cybercrime prohibited by law nor a law enacted against cyber-crime. Lack of punishment reduced the expected cost of the criminals, which were composed thus of moral costs and substantial costs, specifically, the perpetrators' necessary devices and labor in cybercrime. Because there was no cybercrime law, there was neither expected punishment nor the expected cost induced by the expected punishment. Under such circumstances, the probability of conviction equaled zero. The expected utility of the perpetrator almost equaled the utility of a situation in which crime went undetected or unpunished. After that years passed, the number of computers increased and so was the increase in the number of the cyber crime. After the year 2000 there was rapid rise in the internet. Computer crime and relevant legislation was globalized, expanded from developed countries to less developed countries and to developing countries. Law enforcement also took a series of measures against cyber-crime.[1]

Latest Stats of Cyber Crime

- Internet subscribers in India crossed the 400 million mark, and are expected to reach 462 million by June 2016. Cyber crimes reported in India rose 19 times over the last ten years (2005 to 2014), from 481 in 2005 to 9,622 in 2014, and India is now ranked third – after the US and China – as a source of *"malicious* *activity"* on the Internet and second as a source of *"malicious code"*. Arrests involving cyber crimes also rose nine times from 569 in 2005 to 5,752 in 2014, according to National Crime Records Bureau (NCRB) data, even as more Indians logged on to the Internet. Though the latest reports tell that Overall malware activity decreased in June, down almost 13 percent from the previous month.

- Financial Trojan activity decreased for the fifth consecutive month in June, down 16 percent from May.
- Ramnit keeps the number one spot when it comes to financial Trojan activity in June, accounting for 62.9 percent of all activity. Zbot retains second place this month, with 19.8 percent of all activity.
- Ransomware activity decreased again in June, down 13 percent from the previous month. This marks the third month in a row to see a drop in activity.
- Downloader activity decreased in June, down 8 percent from May. Web attacks decreased by 7 percent in June. This is the first month to see a drop in activity since February.
- The most common user names used in attacks included "admin", "root", and "default", while "123456", [BLANK], and "admin" were the top three passwords.
- Like jacking topped the list of social media scam types, followed by fake offers.
- The email malware rate decreased in June to 1 in 654 emails. This is the fourth consecutive month to see a decrease.
- At 1 in 230 emails, Mining topped the list of industries receiving malicious email in June. Wholesale Trade came in second place with 1 in 404 emails being malicious.
- Finance, Insurance, and Real Estate topped the list when it came to industries receiving phishing email, with 1 in 5,711 emails, down from 1 in 17,195 emails the previous month.
- The Finance, Insurance, and Real Estate sector also saw the highest spam rate in June at 58.2 percent.
- The phishing rate increased in June to 1 in 8,516 emails, up from 1 in 15,098 the previous month.[2]

Even though the latest reports show that some of the threats from online are declining but they studies shows that the new threats keep coming like some of the recent threats are Unofficial telegram app secretly loads infinite malicious sites and over 150 jio apps offer free data but deliver only ads.

These are not only some of the issues which are faced by the India but there are certain other things like Obscenity, Cheating, Sexual Exploitation, which are leading cybercrimes in India. As many as 758 cases were registered for publication or transmission of obscene or sexually explicit content under the IT Act. Cheating (1,115) was the most reported crime, accounting for nearly 50% of IPC crimes. Under SSL offences, copyright violation was the most reported crime (118 of 149)."Greed/financial gain" were the major motives behind cyber-crime cases in 2014 with 1,736 cases, followed by "insult to modesty of women (599)", fraud or illegal gain (495), sexual exploitation (357) and "personal revenge/settling scores (285)".Maharashtra reported the most cyber crimes (1,879) in 2014, double the cases (907) of the previous year. Uttar Pradesh was second (1,737), followed by Karnataka (1,020), Telangana (703) and Rajasthan (697). The top five states accounted for 63% of all cases in 2014. As many as 5,752 people were arrested for cyber crimes in 2014, of which 5,744 were Indians and eight foreigners. As many as 95 persons were convicted and 276 acquitted for cyber crimes in 2014.[3]

There is a need of kaws for the internet because Systems across the globe have many different rules governing the behavior of users. These users in most of the countries are completely free to join/leave any system whose rules they find comfortable/not comfortable to them. This extra flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult for System Administrators to have a check on Frauds, Vandalism or Abuses, which may make the life of many online users miserable.[4]

Why developing countries undergo more damage due to cyber crime as compared to developing countries?

Few experiences undermine a digital financial services (DFS) customer's finances and trust in DFS like becoming the victim of a cybercrime. This is especially true of low-income customers, who are least able to rebound from the losses, and of the newly banked, whose trust in financial services may be fragile.

Unfortunately, cybercrime is a growing problem in developing countries, where customers often conduct financial transactions over unsecure mobile phones and transmission lines that are not designed to protect communications.

In Africa, the number of successful attacks against the financial sector doubled in 2017, with the biggest losses hitting the mobile financial services sector. DFS providers must adopt stronger cyber security measures to protect themselves and their customers. But which threats pose the greatest risk today?

In 2017, CGAP surveyed 11 DFS providers operating in Africa to understand how they perceive and mitigate cyber risks. We learned that all of them have been affected by cyber security incidents and are at various stages of implementing cyber security measures in their organizations.

While they are still most concerned about better-known types of fraud in DFS, such as malicious employees and agents, they are seeing themselves confronted with four types of risks emerging in cyberspace.

Social engineering

In a social engineering attack, the criminal tricks the victim into revealing sensitive information or downloading malware, which opens the doors to physical locations, systems or networks. The idea is to exploit a vulnerable person rather than a vulnerable system. DFS providers from Ghana, Kenya, Tanzania, Uganda and Zambia told us that fraudsters had duped their employees into sharing their user login details and then accessed corporate information systems.

Most DFS providers consider careless or unaware employees to be a major factor in their organization's cyber risk exposure. But DFS customers are a vulnerability, too. The newly banked are more likely to fall victim to this type of scheme because of their limited experience with digital fraud.

Providers can guard against social engineering through regular awareness and education campaigns. It is also important to appropriately manage user access rights, introduce system log monitoring processes and require two individuals for completing sensitive transactions (i.e., maker-checker controls).

Data breaches

Using malware or social engineering, hackers can gain access to valuable information, such as credit card numbers, customer personal identification numbers, login credentials and government-issued identifiers. Weak patch management, legacy systems and poor system log monitoring were cited as the main reasons why DFS providers' systems are susceptible to hacking attacks.

In addition to financial losses that can result from a data breach, providers' reputation and customers' trust are at risk. In 2017, thieves breached a DFS provider's systems in Kenya and stole hundreds of customers' identities. The fraudsters accessed sensitive customer information, such as account types and last transactions, which allowed them to pass as legitimate customers and apply for loans in the victim's name.

To protect against data breaches, DFS providers need to regularly update their systems and software, patch their systems, use strong encryption for data at rest and in transit and implement 24/7 system log monitoring.

Outages and denial of service attacks

DFS providers sometimes experience system outages during routine system upgrades or patches. Earlier this year, an upgrade gone awry left DFS users in Zimbabwe without access to their digital money for two days. Systems unavailability can also be the result of a cyber-attack.

For example, in 2017, M-Shwari customers in Kenya were left without access to their savings and loan products for five days. And, after the outage, several found inconsistencies in their account balances. The most frequent form of attacks that cause system unavailability are denial-of-service attacks.

In a denial-of-service attack, cyber criminals overwhelm a server by flooding it with simultaneous access requests, depriving legitimate users of access to the system. In most cases, the objective is to harm the business. Yet, in some cases, cyber criminals have launched denial-of-service attacks to distract attention from an attempt to gain access to the system.

Effective countermeasures include continuous network traffic monitoring to identify and detect attacks while allowing legitimate traffic to reach its destination, a solid and tested incident response plan that allows for quick reaction in an emergency and strong change management processes and disaster recovery planning.

Third-party threats

DFS providers rely on third parties for a range of services, such as mobile network, information technology and data storage solutions. Sometimes, these providers misuse their system rights to access confidential customer information that they can sell or use for social engineering.

Also, a third party that handles sensitive information may not have appropriate safeguards against cyber-attacks, putting at risk the confidentiality and integrity of the DFS provider's customer data.

To address third-party threats, DFS providers should implement due diligence reviews of current and potential partners, including reviews of their security policies and practices.

Impact on low-income customers

If physical money used to be kept safe in bank vaults, what is protecting money now that it is digital? This is a financial inclusion question because the answer is especially important for low-income customers. In developed countries, it is usually the financial services provider that is legally responsible for bearing the cost of fraud. In developing countries, it is often the customer.

The experience of fraud and rumors of fraud experienced by others causes mistrust in DFS, especially among lower-income consumers. The DFS providers we spoke with in Africa recognize their need to invest more in cyber security for both themselves and their customers. They acknowledge that better safeguards are needed to mitigate threats and be better prepared to respond to incidents.

Failure to take the relevant steps could deter people from entering the formal financial system and significantly harm consumers and markets.[5]

Need for Cyber Laws

The above stats clearly tells us that there is a need of stricter cyber laws and how that can be solved?

- There is a grave need of new laws to protect us from the internet and for that cyber cells should be made more informative about the virus and malware attacks.
- They should be made more responsive for the certain keywords, so that if there will be any cybercrime happening in the sites, they will know about.
- There is also an issue that if our administration gets to know about cybercrime, but due to lack of evidences these cases take a longer time to be solved this happens because many IT giants servers are not situated in India so retrieve that information, they have to go through the IT giant country's legislation which takes a hefty time.
- There is need of certain international legal framework, which will bring all the countries together and will help to share the securities, ways to disinfect and the data. As it will help to safeguard to secure the data in uniform manner.

Even after implementing the laws there are things which should be done like.

- Regular check of threats at global level.
- Letting people know about the sites containing malware or virus.
- Blocking of new miscellaneous sites.
- If cyber-crime is reported by someone, immediate checks should be done on that site.

To meet the challenge posed by new kinds of crime made possible by computer technology including telecommunication, many countries have also reviewed their respective domestic criminal laws so as to prevent computer related crimes. Some of these countries are USA, Austria, Denmark, France Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, UK, Malaysia and Singapore.

However even after reviewing the laws the developed countries like USA stands at the second level which is prone to cyber-attacks.

Conclusion

Cybercrime or hacking kind of things that are really hard to be controlled, even though developed countries are less prone to this kind of attacks but they are also no fully secure. USA introduces 5 new laws to prevent from cybercrime but it's still happening, Only thing is they are well informed which sites are to be taken down to prevent crime. But in the case of developing countries most the time they are hacked and all their data is being sold also but they don't even get to know because they are lacking the security of the systems and through checks are not being done to prevent them on a regular basis. There is a need for international laws and treaties so that the cybercrime can reduced to a certain level. Or it will keep spreading like fire and the developing countries will not even know about, controlling them will be secondary.

References

1. Xingan Li Johannes, Cyber Crime and Legal Countermeasures: A Historical Analysis Sascv. org (2019), https://www.sascv.org/ijcjs/pdfs/LIijcjs2017vol12issue2.pdf (last visited Jul 16, 2019).
2. https://www.symantec.com/security-center/threat-report
3. http://ncrb.gov.in/
4. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005846.pdf
5. http://www.ipsnews.net/2018/10/cyber-attacks-growing-problem-developing-nations/