CYBERCRIME IS THE BANE OF THE INTERNET: IS INDIA READY?

By Aarushi Chopra
From Amity Law School, Noida

Scope of the Article

Statement of problem:

This article highlights the issue of the increasing threat of cybercrime in India with main emphasis on whether India is still ready to deal and tackle with this growing menace and what steps have been taken place by the Indian government to deal with this situation proactively.

Limitations:

Over the span of approving and examining resources that the researcher has depended upon, it has been unequivocally felt that the ambit of this zone of law is still under development, particularly in India

Introduction

Cybercrime is the bane of the internet and new technologies generate new opportunities of more innovative ways of doing crimes and this threat is growing multi fold in this new world of digitization and growing technology. As the world is becoming digital, crime is also moving towards virtual space from physical space. It is going through a massive change in its modus operandi and it is going to multiply whether we like it or not. According to a study from the University of Maryland, there is a cyberattack once every 39 secs. This shows how the technical evolution have outpaced the defence as well as security tactics of private organisations and the governments all over the globe.

We are in this digital age where our virtual identity has become an important aspect of our day to day lives. We are now just a bundle of numbers or codes in numerous computer databases owned by corporations and government. With the evolution of cyberspace which is taking place at an unprecedented pace, especially in the developing economies, the exploitation of it by utilising it in it's true essence has made people generate millions and millions of dollars. Earlier, cyberthreats were hardly of any value but now when we see it, it is disruptive and has become rather destructive. So with the scale of cyberattacks increasing with each passing day, not only India but all countries across the globe cannot afford to ignore this threat.

What is Cybercrime?

Cybercrime refers to all the illegal activities carried out by using technology as an instrument. It is a criminal act which targets a computer, network device or a computer network.

An important feature of cybercrime is its nonlocal character: acts can be done in jurisdictions which are separated by vast distances. This is also a severe problem for law enforcement since international cooperation is needed for previously local or even national crimes now. For example, if a person uses his computer to access child pornography in a country which does not ban child pornography, then is that particular individual committing a crime in a country where such data is illegal? Where will cybercrime exactly take place?

Types of cybercrime:

Cyber criminals are professionals who are very organised and use advanced techniques. Others are just some novice hackers. Hence, Cybercrime attacks can commence wherever digital data exists, along with an opportunity and motive. Cybercrimes do not really occur in a vacuum but are in fact distributed in nature. Therefore, cybercriminals mainly rely on various other actors to finish the crime for them like a malware creator who uses the dark web to sell the code. They use numerous attack vectors for the cyberattack and are constantly developing to new techniques for achieving their goals without getting detected or arrested.

Most cybercrimes fall under the following two categories:

I. Crimes that targets computer networks or devices (example: to gain access to a computer)
II. Crimes using computers as an accessory to a criminal act (example: online identity theft used to steal funds from a bank account)
III. Crime using computer as a weapon for an attack (for example: DoS attack -denial of service)[1]

Cybercrimes can be mainly bifurcated into the following 3 kinds:

A. Cybercrime against persons (cyber harassment, online libel or slander, child pornography, identity theft, spoofing, credit card fraud)
B. Cybercrime against property (DDOS attack, hacking, theft of IP, computer vandalism, computer squatting, virus transmission)
C. Cybercrime against nations (cyber warfare, cyber vandalism)

The following are some standout cybercrimes to watch out for:

1. Internet and email fraud
2. ATM fraud
3. Wire fraud
4. Software piracy
5. Botnets
6. PUPs
7. Exit scam
8. Cyberextortion (demand of money to prevent a threatened attack)
9. Ransomware attacks (is a type of cyberextortion)
10. Crypto jacking (mining of cryptocurrency using resources not owned by hackers)
11. Cyberespionage (access of company or govt data by hackers)

Taking the example of **Equifax, an American credit monitoring company** was hit by a massive data breach which impacted over 143 million customers. The attackers found a vulnerability in Equifax's open source software which allowed them to access all the sensitive files of the company. The data stolen not only included full names, birth dates, social security numbers, addresses but also included around 200,000 credit card numbers and 200,000 additional documents that contained personal-identifying information. Even the way in which the breach was handled was widely criticized which shows how there is a real need for notification procedures for breaches. Another example is the **Uber breach** where hackers stole personal data of around 57 million riders and drivers. Uber paid the attackers $100,000 to keep the data safe and to keep quiet about the breach. The data stolen included names of the riders and drivers, their phone numbers and email addresses. Even the driver's license of some drivers were stollen.

With the rapid increase in cybercrimes all over the world, it has become a major threat to all those who use the internet, with millions of user's data stolen over the past

[1] *"Cybercrime types, examples, and what your business can do"*, exabeam, https://www.exabeam.com/information-security/cyber-crime/

few years. This has created a major dent in many economies.

Is India Ready?

As India embarks on its journey to Digital India, the challenge to address the issues of cybersecurity needs to take place on a war footing basis. Even companies are now opting for cyber insurance policies. In fact, according to the DSCI report, around 350 cybersecurity policies have been sold to Indian companies till 2018, which is an increase of 40% from those in 2017.[2] But certainly isn't not enough since these insurances can help cover losses only to some extent and at the end of it the impact of data breaches are not solely confined to monetary losses.

The government of India has attempted to form a cybersecure nation for all is citizens and businesses. They had decided to launch an updated version of the National Cybersecurity Policy this year (2020), which is all ready and will be announced to the public soon as said by the National Cybersecurity Coordinator Mr. Rajesh Pant at an Assocham event. There were also a few initiatives taken by the Indian government in 2019 towards drafting of the above mentioned policy:

1. **CERT-in: Indian Computer Emergency Response Team**
   It is the National Agency developed to handle the country's cybersecurity. It became operational in 2004 and its basic aim is to respond to any computer security incident when they occur, report its vulnerabilities and to promote IT security practices.

2. **NCIIPC: National Critical Information Infrastructure Protection Centre**
   It was created by the central government under Sec 70A of the Information Technology Act, 2000 to protect information infrastructure for critical sectors of the nation from unauthorised access, use, modification, disruption, disclosure, etc. which include: power and energy, telecom, transport, BFSI, strategic and public enterprises.

3. **Cyber Surakshit Bharat**
   The Ministry of Electronic and Information Technology (MeitY) launched this initiative to spread awareness about cybercrime, build capacity and enable government departments on steps to be taken for creating a cyber resilient IT set up. It also aims at conducting workshops for citizens as well as businesses to educate them on the cybersecurity practices that can be taken place.

4. **Cyber Swacchta Kendra**
   The Ministry of Electronic and Information Technology (MeitY) launched this initiative. It is a cleaning bot used for analysing malware and detecting botnot infections. It also aims at notifying, enable cleaning and secure systems to prevent further infections.

5. **Personal Data Protection Bill, 2019**
   This is the most important initiative taken by the Indian government. As the name suggests, this bill aims to protect the personal data of individuals in India from being

[2] *Shomiron Das Gupta***,** Is India Cybersecurity - Ready In 2020?, Silicon India, https://startup.siliconindia.com/viewpoint/ceo-insights/is-india-cybersecurity-ready-in-2020-nwid-23052.html

processed by government, companies incorporated in India, foreign companies. It also aims at establishing a Data Protection Authority for the same.

India also has an Information Technology Act, 2000 (IT Act) which deals with cybersecurity and cybercrimes. This act provides protection for transactions taking place through electronic interchange and electronic communications. It also aims at safeguarding electronic data, information, records, and prevent any kind of unlawful or unauthorised use of a computer system. Cybercrimes like hacking, phishing, denial-of-service attacks, malware attacks, electronic theft and identity fraud are specifically punishable under this act.

There are also some relevant rules which are framed under the IT Act like:

i. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules). It recommends reasonable security practices and procedures which can be implemented for collecting as well as processing personal or sensitive personal data.

ii. The Information Technology Intermediaries Guidelines Rules, 2011, under which intermediaries are required to implement reasonable security practices and procedures for making their computer resources and information contained in them secure.

There are other laws too that contain provisions related to cybersecurity which includes the Indian Penal Code, 1860 (IPC) which punishes offences such as defamation, cheating, criminal intimation and obscenity even including the ones committed in cyberspace, and then we have the Companies (Management and Administration) Rules, 2014 (the CAM Rules) which are framed under the Companies Act, 2013 requiring companies to make sure that all security systems as well as the electronic records are safe and secure from any unauthorised access or tampering.

Furthermore, there are also some sector-specific regulations like the Reserve Bank of India (RBI), the Department of Telecommunication (DOT), the Securities Exchange Board of India (SEBI) and the Insurance Regulatory and Development Authority of India Act, 1999, who have mandated certain cyber security standards that are to be maintained by their regulatory entities like banks, telecom service providers, insurance companies and other listed companies.

Though India has taken a few steps and is still taking more towards strengthening its cybersecurity, it still needs to invest more around this area, as these aforementioned initiatives and laws can only help to an extent. Strong legal foundation and policies is the need of the hour. While we are working on Digital India, we also need to work more on cyber safety by making the government, private institutions and educational institutions work together. Policies made by the government should endure that both public and private entities are equipped enough to tackle any challenges of cybersecurity. Private entities invest huge amounts on finding solutions but it is needed to be understood with the help and support from the government which will make them well equipped to deal with such incidents.

Besides all this, what also needs to be looked into is the regulation of the role of software developers and software product companies. Such companies are pushing software with evident vulnerabilities which is easily exploited by cybercriminals. What is even more important is the speed and agility that is there while we counter these crime. So to stay one step ahead of the attacker, one needs to continuously adjust and improve and the technology needs to constantly evolve.

Conclusion:

India is still way far behind and has to catch up if it wants to be at par with other developed countries on readiness parameters of cyber security infrastructure. More serious initiatives need to be taken with a more focused and well-defined approach along with a skilled cyber team. Since cybersecurity is of national importance, there is a need for more public awareness-raising campaigns and education so as to promote the training of needed specialists in cybersecurity. Finally, considering the global nature of cyber threats, it is important to note that cybersecurity cannot be addressed in isolation and an international approach also needs to be sought. The key elements to achieve an effective approach in cybersecurity is the coordination as well as collaboration between various governments and private sector entities from around the globe. India has entered into various cybersecurity related bilateral agreements with various countries and we hope more such agreements will be signed soon.

To make Digital India crime free, we need a two-pronged approach, where firstly, we establish a nationwide hygiene campaign to pre-empt attacks likely to occur due to human error and secondly, we need to strengthen existing laws and enforce them procedure on security agencies. Therefore, with sufficient amount of nationwide awareness on cybersecurity, strong policies and initiatives, India will definitely be able to fight major cyber threats more efficiently and effectively, avoiding heavy damages.

References:

1. "*Cybercrime types, examples, and what your business can do"*, exabeam, https://www.exabeam.com/information-security/cyber-crime/

2. *Shomiron Das Gupta*, Is India Cybersecurity - Ready In 2020?, Silicon India, https://startup.siliconindia.com/viewpoint/ceo-insights/is-india-cybersecurity-ready-in-2020-nwid-23052.html

*****