Cyber Security: An Innovative Safeguard in Digital World

[a] Taruna Malhotra, [b] Mona Malhotra,
[a] Sr. Assistant Professor, Vaish College of Education, Rohtak, India
[b] Assistant Professor, Gaur Brahman College of Education, Rohtak, India

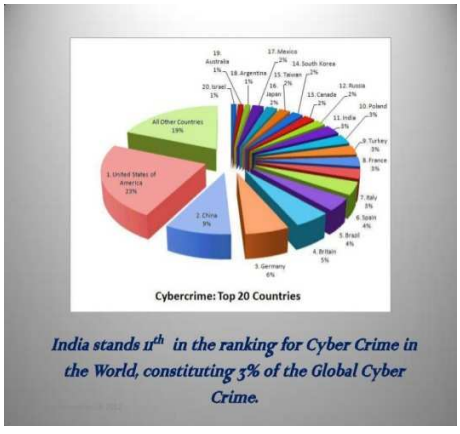
Abstract

"It is only when they go wrong that machines remind us how powerful they are"
-Clive James

In present scenario, we live in a connected world. From the ordinary to the extraordinary, networks and connectivity control our day, keep us running and help us along with our professional and personal endeavors. But on the other hand, this connectivity has a dark side too; as our networks are vulnerable to intrusion by a myriad of actors, including cyber criminals, rogue nation states, hackers seeking to make a political point, cyber terrorists and others with malicious intent. Cyber crimes cover crimes 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.
In the increasingly digital world with an ever-growing e-commerce sector, cyber security is of vital importance. Cyber security involves protecting computers, networks, programs, and data from cyber threats. It is used to refer to the securities offered through on-line services to protect our on-line services. The present paper highlights the need to maintain having a cyber security which is the dire need of the hour.

INTRODUCTION

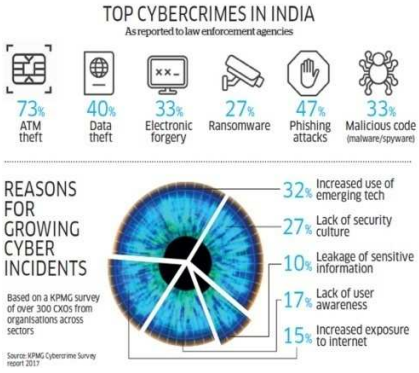
Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or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



In its 2016 cybercrime report, RSA noted that 45% of all online transactions in 2015 were made via mobile channels whereas 61% of attack attempts were made with the use of mobile devices. Additionally, the report mentioned a tremendous 173% increase in this kind of attack that was observed between 2013 and 2015.

WHAT IS CYBERSECURITY?

Techopedia explains , "Cybersecurity is a very broad category which encompasses numerous hardware and software technologies, and can be applied on any level, including personal, corporate or governmental devices or networks."



Cyber security can help protect privacy and prevent unauthorized surveillance and use of electronic data. Examples of cyber attacks include worms, viruses, Trojan horses, phishing, stealing confidential information, and control system attacks. Because of it loose definition; it is hard for the government to regulate how businesses should protect their systems and information. A number of different measures are used to ensure at least a basic level of cyber security. As commonly used, the term "cyber security" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associated field of professional endeavor, including research and analysis, aimed at implementing and those activities and improving their quality.

Cyber security is thus more than just information security or data security, but is nevertheless closely related to those two fields, because information security lies at the heart of the matter.

WHERE INDIA STANDS IN CYBER SECURITY

In India, we have a very high density cyber usage, but an extremely low level of awareness on cyber security. The current cyber security scenario in India can at best be described as reactive. While most of the advanced nations included cyber security as a key socio-political agenda quite some time back, we have been lagging behind in even setting up a national cyber security architecture.

As a nation, we are at the first stage of digitization which pertains to migration of our basic services towards digital platforms. Over the past few years, we have seen tremendous pace in this initiative.

Today almost all our services have become online. However, the situation today demands a parallel focus on securing digital information assets that it creates. Cyber security should be an integral part of all digital initiatives of the Government.

India is at the 23rd slot out of 165 nations in a global index that traces the commitment of nations across the globe to cyber security and helps them to identify areas for improvement. India scores 0.683 and has been listed in the "maturing" category, which includes 77 countries that have commitments towards cyber security and engage in cyber

security programs. Singapore tops the Index with a score of 0.925. India stands 4th in the list of countries for cyber security.

INDIA'S SUSCEPTIBILITY ON CYBERSPACE

With the growing adoption of internet and smart phones, India has emerged as "one of the favourite countries among cyber criminals. India remains vulnerable to cybercrime and cyber-espionage. One more reason is lack of coordination among different agencies. There is growing threat from online radicalization. Moreover attackers can gain control of vital systems such as nuclear plants, railway transportation or hospitals that can subsequently leads to dire consequences.

Countries attack each other to steal sensitive information, and criminals fool customers into giving them financial information. This shows the impact that hacking can have.

- Recent increase in hacking events, from phishing attacks on 26 Indian banks.
- An increasing number of Indians are going digital and doing transactions online, and these hacking incidents expose the country's cyber security vulnerabilities
- There has been a surge of about 350% of cybercrime cases registered under the Information Technology (IT) Act, 2000 from the year of 2012 to 2016.
- As more Indians embrace online banking, criminals are following them online
- Another trend is the increasing no. of attacks designed for mobiles

NEED FOR CYBER SECURITY

- To ensure critical infrastructure system donot collapse under any situation.
- To ensure Business continuity
- For the success of government initiatives like Digital India, Make in India and Smart Cities.
- To balance individuals rights, liberty and balances.

HOW DOES CYBERSECURITY WORK

Cyber security helps to prevent against the risks associated with any cyber attack, which depend on three factors:

- **Eliminating the threat source:**

  Determining who is attacking can indicate what kind of information or advantage they are seeking to gain. Cyber attacks may be carried out by criminals, spies, hackers, or terrorists, all of whom may do it for different reasons.
- **Addressing vulnerabilities through improving software and employee training:**

  How people are attacking is important in trying to set up the best cyber security possible. This can be likened to an arms race between the attackers and defenders. Both try to outsmart the other as the attackers probe for weaknesses in their target. Examples of vulnerabilities include intentional malicious acts by company insiders or supply chain vulnerabilities that can insert malicious software.
- **Mitigating the damage of an attack:**

  A successful attack may compromise confidentiality, integrity, and even the availability of a system. Cyber theft and cyber espionage might result in the loss

of financial or personal information. Often the victims will not even be aware the attack has happened or that their information has been compromised. Denial-of-service attacks can prevent legitimate users from accessing a server or network resource by interrupting the services.
Some Cyber security technologies are :

- **Firewall:** a network security system to control incoming and outgoing network traffic. It acts as a wall or barrier between trusted networks and other untrusted networks.
- **Anti-virus software:** used to detect and prevent computer threats from malicious software.
- **Intrusion Prevention System:** examines network traffic flows to prevent vulnerability exploits. It sits behind the firewall to provide a complementary layer of analysis.
- **Malware scanners Software:** regularly scans files and messages for malicious code.
- **Encryption:** involves coding information in such a way that only authorized viewers can read it. This involves encrypting a message using a somewhat random algorithm to generate text that can only be read if decrypted. Encryption is still seen as the best defense to protect data.
- **Cryptography:** It is used in two main ways in information security. The better known is to provide confidentiality by encrypting stored data and data in transit.
- **Secure Socket Layer (SSL)**: It is a suite of protocols that is a standard way to achieve a good level of security between web browser and websites.

IT'S TIME FOR INDIA TO UPDATE ITS CYBER SECURITY POLICY

India is transforming itself from an analogue society to a digital nation: everything from financial, utilities, governance and civic services, home security to entertainment and, why, even one's own identity is digital. In such a scenario, national security cannot be divorced from cyber security, cyber attacks and cyber warfare. For long, we have looked at cyber security as simply an issue of protection of specific digital devices against a malware or a virus. It is to an extent, but it is also much beyond that. India is a growing economy, and it's only a matter of time before India starts leaving its digital footprints on the global stage. The time is also right that India recognizes cyber security as the fifth dimension of warfare and accord cyber security the priority it deserves. It's time India declares its public and private digital infrastructure as a strategic national asset. India announced its first ever national-level Cyber Security Policy in 2013, against the backdrop of revelations of NSA surveillance. Now, four years after its inception, the government needs a new policy that outlines a specific framework towards implementing broad principles outlined in the 2013 policy.

In the last four years since the announcement of the Cyber Security Policy, India's cyber landscape has witnessed growing digitization as part of the Government's Digital India push, as well as more sophisticated cyber threats, particularly the Wanna,

Crypt and Petya ransom ware attacks that hit Indian networks this year. These radical changes necessitate an update to India's policy on Cyber Security.

Every IT worker needs to be involved in protecting and defending apps, data, devices, infrastructure and people. Cyber security, a complex domain with constant flux and rapid changes, wants skilled professionals having expertise in mathematics, statistics, data science and computation in order to keep up with the latest challenges in the form of attacks, crimes and frauds.
The government has identified following objectives for securing country's cyber space:

- preventing cyber attacks,
- reducing national vulnerability to cyber attacks
- minimizing damage and recovery time from cyber attacks.

The initiatives taken by the government of India have focused on threats to critical information infrastructure and national security, adoption of relevant security technologies, information security awareness, training and research. Due to dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time. There have been some steps taken:

- The **Information Technology (Amendment) Act 2008** has been enacted to cater to the needs of National Cyber Security.
- Indian **Computer Emergency Response Team (CERT- In)** has been operational as a national agency for cyber security incident response.
- Growth and application of **digital signature certificates** in a number of areas has taken place.
- **National Crisis Management Plan** for countering cyber attacks and cyber terrorism has been prepared and is annually updated.
- **Security Auditors** have been empanelled for conducting security audits

CONCLUSION

With the huge growth in the number of Internet users all over the world, the security of data and its proper management plays a vital role for future prosperity and potentiality. A strong cyber security infrastructure of India is need of the hour especially when there is no well settled international legal issues of cyber attacks that can be invoked in the case of a cyber incidence. It is very important that international legal issues of cyber attacks must be resolved by various government and non government stakeholders. Cyber security is equally important for local, state, and central government as these organizations maintains a huge amount of confidential data and records concerning the country and its citizens.

India has started many good initiatives and formulative far reaching policies in the field of cyber security. However, their actual implementation is still missing and therefore making all these efforts futile. Threat to any single country can jeopardize the very survival of entire world, so we need a national as well as international shift in thinking on cyber security; we need to strengthen the cyber culture. It only takes one person to click

or open a document with malware to let the adversaries into our networks. Change must happen. The government should provide a platform for creating a knowledge repository of cyber incidences where organizations can share their experiences to be able to defend against future cyber events. The cyber security challenges in India would increase in the future as India has adopted the Digital India initiative and India must be well prepared to deal with the same. We should have backup of important data. Our devices should be protected by passwords and there should be restricted access to sensitive data on our devices. And above all, we should aspire for more computer literacy to understand the safety issues related to our cyber space. At the same time we need to utilize the specialization of private sector in the field of cyber security and government should promote more innovative projects for the national cyber space.

References:

- "James Clive". Cyber Security Summit. October 12, 2016. Retrieved 27 February2017.
- http://economictimes.indiatimes.com/articleshow/62489823.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- http://tech.economic times.indiatimes.com/news/technology
- http://economictimes.indiatimes.com/tech/internet
- http://www.microsoft.com/en-us/research/academic program
- KPMG cybercrime survey report 2017