Survey Paper on Cyber Crime: A Threat to National Security

Priyanka Khosla *
Praveer Dubey**

Abstract

Cyber security is an activity that facilitates in securing information and information systems (data bases, data centers, networks, computers and applications) with appropriate technological and procedural security measures. This survey report pays attention to the general interest as well as the tension that hinders the privacy and the cyber security. It explores and relates how cyber security challenges are also challenges for maintaining privacy as well as protection of data. It also highlights the way cyber security policy affects privacy and clarifies how cyberspace governance and data security becomes a global issue. Finally, it has given directions to set key policies with a view to generate dialogue on cyber security as an important element of online privacy protection. Firewalls, Antivirus software and other technical solutions that safeguards computer networks and personal data are vital but not sufficient to ensure security. Cyber Security plays a significant role in the overall development of information technology and services provided by internet. "Cyber Security" is the major concern that seeks our attention whenever "Cyber Crimes" is highlighted. Therefore, "National Cyber Security" starts on how fine is our infrastructure to handle "Cyber Crimes".

Keywords: cyberspace; cyber security; cyber stalking; phishing; bombing

I. Introduction

As "cyberspace" has drawn attention to the global communication and information infrastructure, the safety of cyberspace has now become an urgent and high priority for government and corporations worldwide. Cyberspace is "the realm of electronic world that is created by interconnection of networks of information technology and the information available on those networks. It is a technology available worldwide where 2 billion or more people are connected together to exchange information, services, ideas and friendship." The term cyber security is commonly understood as any kind of measures or steps undertaken to secure information available throughout the world and to secure the infrastructure on which the information resides. Advent of internet has given a new outlook to the usage of computer in our day-to-day lives and exposed our lives to the complexities of cyber-crime. The 'borderless' nature and 'anonymous' character of the problem have made cyber security a major concern across the globe. It is being used to carry out multiple forms of cyber-crime *viz.* identity theft, financial fraud, stealing of corporate information, planting of malicious software (malware)/ Trojans, conducting espionage, disrupting critical infrastructures, facilitating terrorist activities, etc.

Priyanka Khosla*
Department of IT
Institute of Information Technology and Management, GGSIPU, Delhi, India
Praveer Dubey**
Department of IT
GL Bajaj Institute Group of Institutions, Mathura, India

A. Types of Cyber crime/attack

The internet frauds that are reported in the country are mostly related to money circulation schemes, cyber stalking, E-Mail bombing, spoofing, theft of debit or credit card information, Salami Attack, Web Defacing, pornography, remittance towards participation in lottery etc

- **Cyber Stalking:** Furtively following a person, tracking his internet chats.
- **Intellectual Property Crime**: Source Code Tampering etc.
- **Salami Attack:** (Theft of data or manipulating banking account) Deducting small amounts from an account without coming in to notice, to make big amount.

- **E-Mail Bombing:** Flooding innumerable number of E-mails in the email-box, to make important message unnoticeable at times or to halt the services.
- **Phishing:** It refers to stealing of sensitive data in Electronic Banking i.e. it includes Bank Financial Frauds.
- **Personal Data Theft:** Stealing private data available on web or social networking websites, personal computer systems and email account.
- **Identity Theft:** Stealing Cyberspace identity information of individual, Hacking the personal identity information or employing phishing techniques.
- **Spoofing:** Stealing the Credentials in friendly and familiar GUI's, Using tools and other manipulative techniques.
- **Data Theft:** Using malicious code like Worms, Trojan Horses, Virus etc to infect computer systems or hacking the computer systems. Employing different methods to install and propagate malicious code.
- **Sabotage of Computer:** Hacking computer with the help of malware.
- **DOS, DDOS Demat of Service**: Flooding a computer with Denial of Service Attacks, DDOS is Distributed DOS attack.
- **Web Defacing:** Infecting the websites by manipulating or adding the spam messages to web pages.
- **Spam and spoofing:** Sending unsolicited emails through manual and automated techniques.
- **Transmitting obscene material:** Transmitting the indecent and nasty content over the social networking websites on web or any kind of electronic media.
- **Pornography:** Publishing pornographic material online on web like on websites, social networking sites etc.
- **Video Voyeurism and privacy violation:** Transmitting personal Video's on web and mobile phones in the form of MMS.
- **Offensive messages:** Sending or publishing the indecent messages over electronic media like email, websites and social media.

B. Cyber Security Challenges

A report released in January 2014 from the World Economic Forum examines the emergence for novel and innovative approaches to raise resilience against cyber attacks and recommends that the failure to successfully protect cyberspace could have a consequence of approximately US$ 2.9 trillion by 2020. However, the challenges for privacy and data protection have become a challenge for data security. The consequence is that Cyber security is by no ways a static issue with an everlasting solution. Following are some of the emerging challenges for data protection and cyber security.

Complexity of the connected environment

Growing sophistication of the threat

Threats are moving to the mobile sphere

The "big data" paradox: is it a bigger risk or a solution?

For many, breach preparedness is still not a priority

C. Cyber Security Policy Developments

Cyber security is an incredibly complex and changing policy issue. No country, organization or individual is ever completely immune to cyber risks, and approaches to protecting against cyber threats can vary greatly depending on the values and decisions that underlie cyber security activities. As the cyber security policy is taken into consideration by the stakeholders, it has become necessary to ensure that the discourse around cyber security includes the acknowledgement of its link to data security on web or on personal systems, faith and privacy.

The following section will consider cyber security policy developments and foreign policy considerations.

Stewardship vs. securitization

As cyber security policy has taken a position at a national level, there is possibly a risk that data security at the national level and public safety objectives could take a leading role in formulating responses to cyber thefts or threats, at the expense of privacy protection. In this manifestation, cyber security policy should

promote – "securitization of cyberspace: a transformation of the domain into a matter of national security." when national security is so often used to rationalize extraordinary intrusions on privacy of individual, it will be imperative to make certain that cyber security approaches and activities do not support building massive surveillance systems for unlimited and endless monitoring and scrutiny of the personal information of individuals. Cyber security efforts should not expand surveillance to the loss of civil liberties, individuals' privacy or other democratically held values. Governments must build in the necessary checks and controls to reflect the privacy norms we ascribe to as a society. As an alternative, Deibert presents an argument for a stewardship approach to cyber security, where "governments, NGOs, armed forces, law enforcement and intelligence agencies, private sector companies, programmers, technologists, and average users must all play vital and interdependent roles as stewards of cyberspace." The concept of stewardship in cyber security acknowledges that cyberspace belongs to no one in particular, but that everybody has an influential role to play in shaping its foundation and a stake in its evolution. This alternative approach recognizes that cyber security is a shared responsibility because of the ways in which cyberspace is interconnected and interdependent, and the role all organizations have to play to ensure that their actions do not introduce security risks into cyberspace in general, or fail to uphold privacy principles. A stewardship approach also calls for accountability on all of the stakeholders involved in cyber security: "Securing cyberspace requires reinforcement, rather than a relaxation, of restraint on power, including checks and balances on governments, law enforcement, intelligence agencies, and on the private sector." As holders of vast amounts of personal information, it is logical to expect that the private sector assume some responsibilities to protect the infrastructure of cyberspace and the personal information that flows through it.

Cyberspace governance and security is a global issue

Given that information flowing through cyberspace is not constrained by national borders, "with whom we share data and where it eventually exists in cyber world is an intrinsic international concern."As such, citizens of every country face similar risks in the fortification of their privacy rights. Issues of cyber security and privacy protection are global challenges that require a global response.

II. Security Training and Awareness

The human participation is the weakest connection in any information security program. Communicating the impact of information security and promoting safe computing are keys in securing a company from cyber crime.

The best practices used to lessen cyber crimes are explained below:

Use an easy "passphrase"—
E@tUrVegg1e$ (Eat your veggies) and make sure to use a combination of lower and upper case alphabets, symbols, and numbers to make it less prone to brute force attacks. Try to avoid simple dictionary words because they are easy target for dictionary attacks – (kind of brute force attack).

Any "passphrases" should not be shared or written anywhere.

Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.

Do not click on links or attachments coming via e-mail from untrusted and unauthenticated sources.

Do not send sensitive business files to personal email addresses.

Suspicious or malicious activities should be immediately reported to security personnel.

Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.

Educate employees about phishing attacks and how to report fraudulent activity.

III. Recommendations

Utilities should endeavor for real-time situational intelligence data of operational technology (OT) systems' security posture. Huge damage can easily

be caused due to attacks on utility OT systems that can effect in loss of money and can reduce customers' confidence in electricity provider. By real time situation data of OT systems, utility can significantly tackle any potential threat in time.

Utilities should recognize that threats can be originated from both either inside or outside of the utility's systems. For example, anyone within the utility's system can execute an internal attack by using a simple USB thumb drive or a malware can be embedded in new equipment.

Both OT and IT systems are susceptible to cyber attacks due to various networks (and silos) across utility systems. Security gaps are left because of multiple networks often having varying degrees of security and often do not integrate with one common system. These gaps can easily be identified by hackers. can with no trouble identify. Thus, utility cyber security systems are supposed to permit integration of OT and IT networks and scale across multiple service territories and systems.

If utilities work together with venders using standards based architecture, it will help them to implement scalable security systems that can work in multiple vendors.

Defense in depth is strongly advocated for cyber security by implementing multiple levels of security to achieve

- Prevention
- Detection
- Identification
- Mitigation

Threats will be evolving continuously, but a multifaceted approach to security is a critical defensive strategy.

OT and IT network convergence are driven by new technologies; specialized representative should be established by utilities or office where security liability for all networks is at topmost priority.

IV. Conclusion

The cyber crime threats are ominous and too real to be overlooked. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thought out Cyber policy, including crisis management in the event of a worst case scenario.

References

1. ThillaRajaretnam Associate Lecturer, School of Law, University of Western Sydney, "The Society of Digital Information and Wireless Communications (SDIWC)",International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)
2. Thomas H. Karas and Lori K. Parrott , Judy H. Moore , "Metaphors for Cyber Security", Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839
3. BinaKotiyal, R H Goudar, and Senior Member, "A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena", IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012
4. Loren Paul Rees, Jason K. Deane , Terry R. Rakes , Wade H. Baker, "Decision support for Cyber security risk planning", Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States
5. Farah J., Mantaceur Z. & Mohamed BA. (2007). "A Framework for an Adaptive Intrusion Detection System using Bayesion Network." Proceeding of the Intelligence and Security Informatics, IEEE, 2007.
6. Booz Allen and Hamilton, Reports, ¯"Top Ten Cyber Security Trends for Financial Services", 2012
7. Ravi Sharma, "Study of Latest Emerging Trends on Cyber Security and its challenges to Society", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012
8. BinaKotiyal, R H Goudar, and Senior Member, "A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena", IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012