IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 23, Issue 8, Ver. 1 (August. 2018) PP 98-100
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Safeguarding privacy and cyber security

Dr. Rashmi Gupta
Lecturer in G.P.E.M. Deptt.
Govt. G.D. Girls College, Alwar, Rajasthan

Abstract
Cyber security associates with technologies, processes and practices designed to protect organization's networks. Today internet and cyber space is the life line of every business and to protect the data present in these networks is a big concern for every organization. Cyber security is basically protecting computer, computer networks, data and information from an unauthorized access, vulnerabilities and attacks by cyber criminals. It also protects the IT infrastructure from Cyber Terrorism, Cyber Espionage and Cyber Warfare. Cyber security has emerged as a strong player to deal with various security breaches and hacking issues in the cyber space, which impacts the economic growth of the organizations. With high profile security breaches and advanced threats, cyber security concerns have influenced the regulatory authorities to bring out necessary regulations. A structure of safeguards is presented, which helps to specify safeguards concurrently regarding function and time. Then, the most common safeguards are explained in detail. Every safeguard is described in order to create an understanding that is focused on the basic characteristics and the intentional use of the safeguards.

Keywords: Vulnerability, Confidentiality, Integrity, Availability, Cyber Terrorism, Cyber Espionage, Cyber Warfare.

I. Introduction

In the modern day, there are dozens or possibly even hundreds of different interconnected assets, networks, and systems that we rely on every day for the normal functioning of society. Without these various infrastructure components, we wouldn't be able to enjoy the benefits of living in the 21st century small-scale disruptions to these components would result in the **temporary loss of crucial capabilities**.

Critical infrastructure security involves identifying, prioritizing, and then providing plans to protect both physical and electronic infrastructures instrumental in the proper functioning of society. By using physical security, such as EMP Shields, and cyber security, critical infrastructure security ensures that a country's government and financial markets can continue functioning unimpeded or with minimal disruption in the wake of either an intentional attack or a natural disaster.

The different infrastructure sectors that fall under critical infrastructure security are varied. However, when regarded together, these sectors make up the majority of any society's ability to function – and the disruption of even one of these infrastructure sectors can have disastrous results for those living within that society. They typically include defense and national security, banking and finance, transportation and supply chains, communications, and healthcare, to name but a few.

Commonly Used Security Safeguards

1.Administrative Safeguards

Access to personal health information and access to any place or system where personal health information is kept must be restricted to individuals who are authorized to use, modify, transform, disclose, dispose or destroy personal health information to perform their assigned duties. Employees and other information users must be authorized to access, maintain, change, use or distribute information. Authorization for each information user should be based on the 'need to know' of that individual.

Physical Safeguards

In addition to restrictions on who can access personal health information, access to the facility, offices, information retrieval equipment and systems and information stores must be controlled to ensure that access is granted only to individuals with authorization for such access. Physical security safeguards to maintain access control can range from anti-theft systems such as bolting equipment to the floor in secure rooms, locked desks and cabinets. protection measures should be applied to personal health information with a high level of sensitivity and with a greater possibility of causing damage to an individual if it is accidentally disclosed, stolen or finds its way into unauthorized hands. investigates the theft of computers that were connected to the electronic medical record system within a clinic.

Technical Safeguards

Identification and authentication safeguards to monitor security systems and procedures may be needed. These include virus scanners, firewalls, monitoring operating system logs, software logs, version control and document disposition certification. “All methods of communication” includes verbal communication, transmission of written documentation, telephone, cellular phone, fax, e-mail, video and audio communication or any other form of electronic communication.

Cyber security Approach

To have a successful Cyber security approach organizations should maintain a balance between accessibility and security. To implement an effective Cyber security program, organizations require few essential parameters, which are:

• Risk Awareness: The foremost and most important parameter is to generate awareness throughout the organization regarding the probable risks, in other words to create a risk-aware culture. It is important for organizations to know about their vulnerable areas, from where attacks can come, what are the security goals and let everyone know about it.

• Powerful Security System: To deal with various attacks and threats, organizations need a robust security rich system, which can track and update all the systems, networks, as well as install the essential software regularly.

• Incident Management: It is important for Organizations to intelligently manage incidents. Application of automated response capabilities and intelligent analytics is the need of the hour for better monitoring and for better incident management.

Skillful Workforce: The organization should have a team of experts which is able to handle the security systems. The workforce should have desired skills, knowledge and should be continuously updated about the risks and threats in the current scenario.

Why is Cybercrime Increasing

Information theft is the most expensive and fastest-growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services.

But it's not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government.

Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations, and their methods of attack on different security systems.

Social engineering remains the easiest form of cyber attack with ransomware, phishing, spyware being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cybersecurity practices are another common attack vector, making vendor risk management and third-party risk management all the more important.

According to the Ninth Annual Cost of Cybercrime Study from Accenture and the Ponemon Institute, the average cost of cybercrime for an organization has increased by $1.4 million over the last year to $13.0 million and the average number of data breaches rose by 11 percent to 145. Information risk management has never been more important.

Data breaches can involve financial information like credit card numbers or bank account details, protected health information (PHI), personally identifiable information (PII), trade secrets, intellectual property, and other targets of industrial espionage. Other terms for data breaches include unintentional information disclosure, data leak, cloud leak, information leakage, or a data spill.

Other factors driving the growth in cybercrime include:

- The distributed nature of the Internet
- The ability of cybercriminals to attack targets outside their jurisdiction makes policing extremely difficult
- Increasing profitability and ease of commerce on the dark web
- The proliferation of mobile devices and the Internet of Things.

II. Conclusion

if organizations don’t follow or implement Cyber security it can lead to financial loss and can also affect the image of the Cyber Security: Safeguarding the Networks 521 organization; the productivity is also affected. The management of the organization should make security policy a part of its strategic planning and every employee of the organization should be aware about the security policies and the probable risks that can affect their performance. The government of India has taken many measures to overcome cyber crime and network security issues but still lots need to be done in this area. Since more and more people are using online services, it becomes essential to educate them regarding cyber crime and how they can deal with it. An awareness needs to be generated amongst the common man so that he doesn’t fall prey to any kind of cyber threat while using computer networks.

References

[1]. IBM Security Services Cyber Security Intelligence Index- Analysis of cyber security attack and incident data from IBM’s worldwide security operations July 2013.

[2]. Jonathan Diamond, India's National Cyber Security Policy in Review, The Centre for Internet and Society, July 2013.

[3]. Department of Information Technology- National Cyber Security Policy of India.