International Journal of Engineering Research and General Science Volume 2, Issue 5, August-September, 2014
ISSN 2091-2730

A Study of Current Scenario of Cyber Security Practices and Measures: Literature Review

Rajesh Mohan More[1], Dr. Ajay Kumar[2]
E-Mail- more.rajeshmore@gmail.com

Abstract— Security measures are of prime importance to ensure safety and reliability of organizations. Hacking of data and information has become almost a routine and regular of organizations. Before we think to combat such a situation; to avoid both predictable and unpredictable loss, danger and risk associated, tangible and intangible factors, we have to strategize in keeping cool in the heat of battle and find out the causes attributing to the same; so proactive action need to be taken to exterminate the same. The researchers feel to encircle parameter to have an in-depth insight such as – integrity of network connections and components, telecommunication issues, firewall, filtering, intrusion detection and prevention system, and network maintenance. These are in fact intra and interrelated.

Keywords— Intellectual property, computer security, security risks, vulnerability, antivirus, encryption, cyber terrorism, auditing, reviewing, intrusion detection system and intrusion prevention systems.

INTRODUCTION

In today's information-age, an organization's dependence on cyberspace is becoming an increasingly important aspect of organizational security. As different organizations infrastructure are interconnected in cyberspace, the level of risk to national security has increased dramatically. The threat to cyber security is growing. Computer systems at colleges and universities have become favored targets as they store same record as bank. In academic institute, malicious software (malware), phishing, infrastructure attacks, social network targeting, and peer-to-peer (P2P) information leakage are daily issues. Most university's financial, administrative, employment-related records, library records, certain research and other intellectual property-related records are accessible through a campus network and hence they are vulnerable to security breaches that may expose the institute to losses and other risks.

CYBER SECURITY ATTACKS

Cyber attack refers to the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Such effects on adversary systems may also have indirect effects on entities coupled to or reliant on them. A cyber attack seeks to cause adversary computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary.

Ponemon Institute presents the cyber crime study which is based on a sample of 56 organizations in various industry sectors in United States. Table-1 shows the statistics of different types of cyber attacks occurred in year 2012 & 2013.

Types of Cyber attacks	2012	2013
Viruses, worms, trojans	100%	100%
Malware	95%	97%
Botnets	71%	73%
Web-based attacks	64%	63%
Stolen devices	46%	50%
Malicious code	38%	48%
Malicious Insiders	38%	42%

Phishing & social engineering	38%	42%
Denial of service	32%	33%

Table-1 – Types of cyber security attacks on organizations

The findings in a report released last year by the Center for Strategic and International Studies (CSIS), "In the Crossfire: Critical Infrastructure in the Age of Cyber war". Based on a survey of 600 IT security managers from critical infrastructure organizations, the report found that 37% believed the vulnerability of the sector they worked increased over the year prior, and two-fifths expect a significant security incident in their sector in the next year. Only one-fifth of respondents to the survey believe their sector to be safe from serious cyber attack in the next five years [7]. Around 10% to 20% of the 100+ incidents recorded in BCIT's Industrial Security Incident Database (ISID) to date have been targeted attacks. The knowledgeable insider is the biggest threat and played a part in a high profile case in Queensland, Australia, in February 2000. A disgruntled employee of a water-utility contractor gained remote access to the utility's control system and managed to release over one million liters of sewage into local waterways [8].

ChiChao Lu [18] in his paper explores the increasing number of cybercrime cases in Taiwan and examines the demographic characteristics of those responsible for this criminal activity. As per the statistic 81.1% were male; 45.5% had some senior high school; 63.1% acted independently; 23.7% were currently enrolled students; and 29.1% were in the 18-23 age bracket, which was the majority group. For those enrolled student cybercrime suspects, the findings show that the percentage of junior high school and senior high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004) of cybercrime suspects in their respective years. The high rate shows that the number of currently enrolled students suspected of involvement in cybercrime is cause for concern.

In a survey of 100 UK organizations conducted by Activity Information Management 83% of the respondents believe that they are under increasing risk of Cyber Attack [Figure 1]. It has been found that the financial and IT Sectors have financial and IT sector has sufficient investment in cyber security as compared to sectors like central government, telecoms and academia.

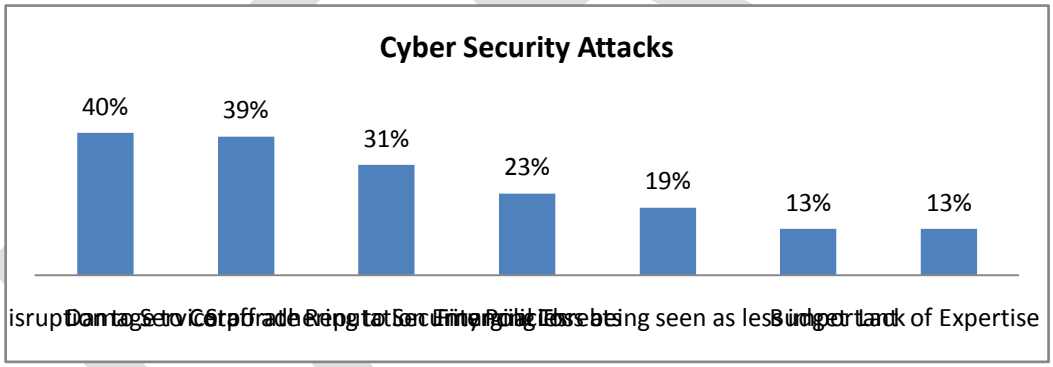

Figure 13 – Percentage of risks due to cyber security attacks

Ponemon Institute has been conducted a survey in June 2011 to study how well the organizations were responding to threats against network security. In a survey it was found that organizations are experiencing multiple successful attacks against their networks [Figure 2]. 59% of respondents said that their organization's network security had been successfully breached at least twice over the past year. According to the findings, the average cost of one data breach for U.S. organizations participating in this study was $7.2 million whereas the average cost of one cyber attack was $6.4 million [15].

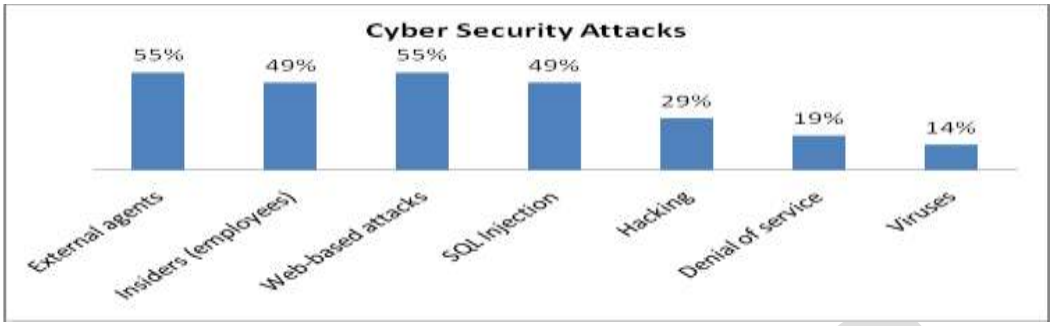

Figure 14 – Distribution of different types of attacks

According to Deloitte-NASCIO Cyber security Study Survey conducted in year 2010; it focuses on initiatives chosen by organizations [Figure 3]. As per as deployment or planning for deployment of variety of security technologies it has been found that more than 80% of agencies have fully deployed antivirus, firewall, and Intrusion Detection and/or Prevention Systems (IDS/IPS), 25% of respondents indicated that they were expected to pilot mobile device file encryption, vulnerability management, and data loss prevention technologies.

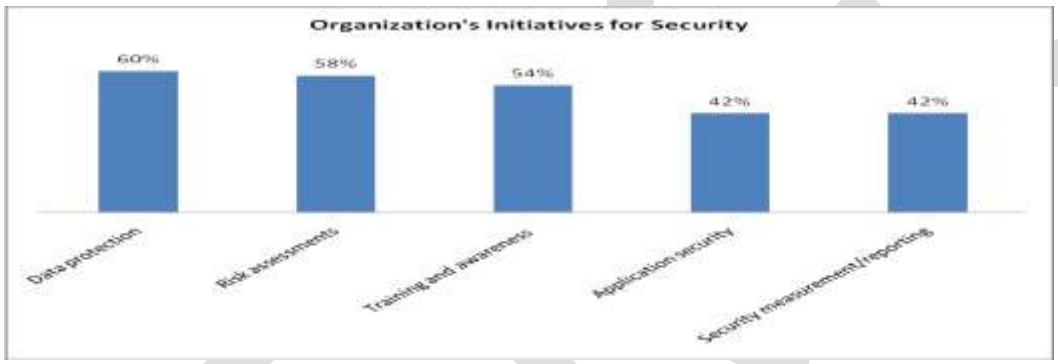

Figure 15 – Organization's initiatives for security

As per as deployment or planning for deployment of variety of security technologies it has been found that more than 80% of agencies have fully deployed antivirus, firewall, and Intrusion Detection and/or Prevention Systems (IDS/IPS), 25% of respondents indicated that they were expected to pilot mobile device file encryption, vulnerability management, and data loss prevention technologies. [16]

According to the CSI Computer Crime and Security Survey conducted in year 2008 of about 522 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities; it has been explored that 53% organizations allocated only 5% or less of their overall IT budget to information security. Figure – 1 shows percentage of the security technologies used by the organizations; it is clearly seen that anti-virus software, firewalls, virtual private network (VPN) and anti-spyware software are mostly used by the organizations. [17]

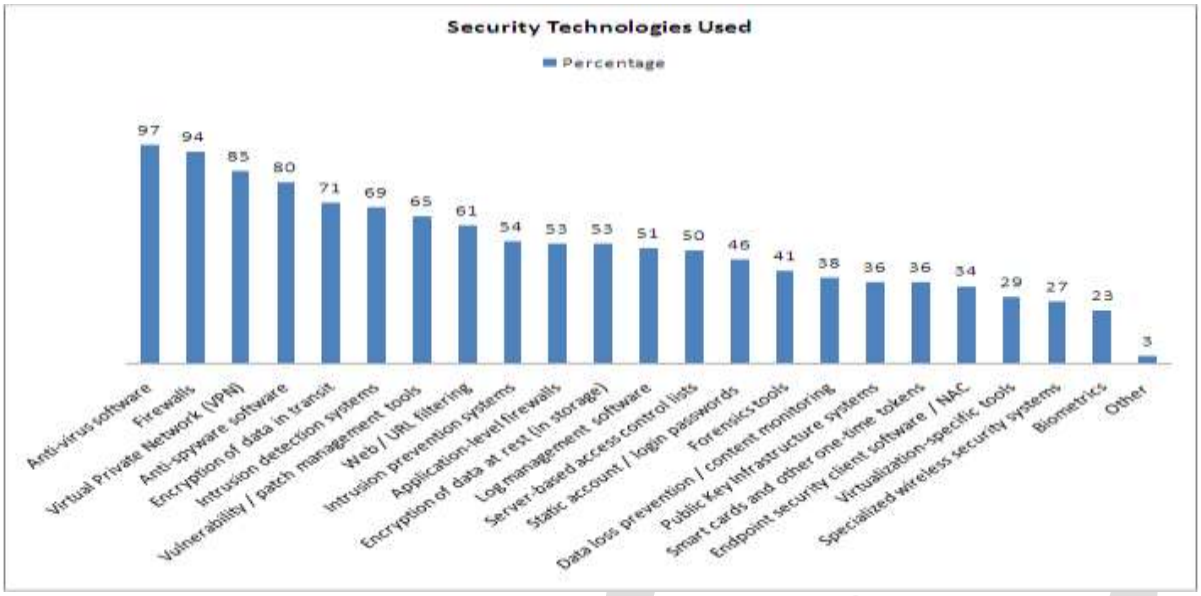

Figure 16 – Security technologies used by the organizations

[Source: 2008 CSI Computer Crime and Security Survey]

The report of the Computer Security Institute (CSI/FBI) (Gordon, Martin, William, & Richardson, 2004) states that nearly 66% of all cyber-security breach incidents, in the 280 organizations who responded to the survey, were conducted from inside the organization by authorized users. Additionally, an overwhelming 72% of organizations reported that they have no policy insurance to help them manage cyber-security risks [12].

Studies by the Computer Security Institute and Federal Bureau of Investigation reported that approximately 90% of respondent organizations in 2001 and 2002 detected computer security breaches [13]. These studies found that the losses averaged over 2 million dollars per organization. In contrast, it was found that companies only spend 0.047% of their revenues on security [14], and this indicates that many firms are not adequately investing in information security.

Cyber terrorism involves leveraging cyberspace as a primary weapon to generate political or social change. It is important to recognize that cyber-terrorism is a tactic that can be used to achieve broader strategic objectives. Jeffrey R. DiBiasi [2] in his study "Cyberterrorism: Cyber prevention vs cyber recovery" undertakes an analysis of the vulnerability of cyberspace to terrorist attacks. The first analysis examines the Code Red Worm and the Slammer Worm were highly destructive and spread faster than normal worms, making them well suited for assessing the existing security of computers and networks. It also examines a staged cyber attack on critical infrastructure, entitled Attack Aurora. In the Aurora attack, researchers from the Department of Energy's Idaho lab hacked into a replica of a power plant's control system. This attack facilitates an analysis of vulnerabilities of critical infrastructures to cyber terrorism.

CYBER SECURITY PRACTICES

Every business relies on information; computers are used to store information, process information and generate reports. Information system assets can be classified by locating information assets and their associated systems as high, moderate, or low impact with respect to the impact of maintaining their confidentiality, integrity, and availability [14]. Computer networks may be responsible for many crucial and back office operations, so it is necessary to secure these systems and their data.

According to the study conducted by Steffani A. Burd [14] following are the statistics of methodologies used [Table-2] by organizations to protect sensitive information.

Security Methods Used	Organizations
Firewalls	94%
Role-based Access	86%
Physical Separation	83%
Encrypt Data on HD	69%
Identity Management	69%
Encrypt Backup Data	63%
Monitor Use of Backup Media	36%

Table-2 – Security Methods Used

Advanced perimeter controls and firewall technologies, encryption technologies, security intelligence systems, access governance tools, extensive use of data loss prevention tools, enterprise deployment of GRC tools and automated policy management tools were the various tools used by these organization. Table-2 shows the statistics of these tools used by organizations in this survey.

Security Technologies	2012	2013
Advanced perimeter controls and firewall technologies	58%	52%
Encryption technologies	50%	48%
Security intelligence systems	47%	45%
Access governance tools	42%	41%
Extensive use of data loss prevention tools	38%	41%
Enterprise deployment of GRC tools	37%	39%
Automated policy management tools	35%	36%

Table-3 – Security Technologies Used

Shannon Keller et al [19] in their paper "Information security threats and best practices in small business" suggests best security practices such as - install and properly configure firewall, update software, protect against viruses/worms/trojans, implement a strong password policy, implement physical security measures to protect computer assets, implement company policy and training, connect remote users securely, lock down servers and implement identity services (intrusion detection).

Society's collective security depends on every user being security-aware and exhibiting thoughtful discipline over his or her personal information and computing resources. It has long been recognized by security experts that the user is in fact the weakest link in the security chain and technical measures alone cannot and will not solve current cyber security threats [6]. "The impact of any given breach can be reduced if there is an adequate audit trail of application activity and a skilled responder who can assist the application team in forensics and root-cause analysis"[5].

According to Jeffrey R. DiBiasi [2] the advanced security procedures, security checklists need to be revised and in some cases created to reflect the most current procedures to prevent and recover from cyber attacks which offer a significant second layer of defense, protecting critical devices from an external or internal attack. Cyber crimes like cyber squatting, internet banking frauds, threatening email, fraud emails etc. shows that really there is need to study and analysis loopholes in current infrastructure. Though cyber law is enacted a much more needs to be done in this area.

Dr Rose Shumba [9], in focuses on the identification of currently used practices for computer security, an evaluation of the practices and reveals the necessity of a public awareness and education program on the importance and relevance of computer security by conducting survey was among 350 multi-disciplinary IUP (Indiana University of Pennsylvania) students. To protect vital

information, the companies must set up a sound security system before the network is intruded which involves identification of the security risks, applying sufficient means of security, and teaching the users data security awareness.

The technology can represent a powerful complement to an organization's networking capabilities. To minimize the security risks, system administrators can implement a range of measures, including security policies and practice [10]. Since security has technology, organizational, and critical infrastructure elements, senior management awareness and commitment is required to develop a control environment that balances the costs and benefits of security controls, keeping in mind the level of risk faced by the organization [11].

Dorothy E. Denning [3] in his paper "An Intrusion-Detection Model" describes a model of a real-time intrusion-detection expert system capable of detecting break-ins, penetrations, and other forms of computer. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expert system. The model is capable of detecting a wide range of intrusions related to attempted break-ins, masquerading (successful break-ins), system penetrations, Trojan horses, viruses, leakage and other abuses by legitimate users, and certain covert channels.

Alexandr Seleznyov, Seppo Puuronen [4] in "Anomaly Intrusion Detection Systems: Handling Temporal Relations between Events" discusses a temporal knowledge representation of user's behavior that is used by data mining tools to construct behavior patterns. These are used to decide whether current behavior follows a certain normal pattern or differs from all known user's behavior patterns. The networked computing offers almost unlimited possibilities and opportunities for intrusions. In this paper they presented an information representation method for intrusion detection system which uses data mining techniques to detect anomalous behavior. The main assumption behind is that the behavior of users follows regularities that may be discovered and presented using the approach for the recognition of the user. The approach suggests that in cases where the audit trail information is inconsistent it is possible to expose it using temporal interval representation applying temporal algebra.

Akaninyene Walter Udoeyop [1] in his study "Cyber Profiling for Insider Threat Detection" introduces a method to detect abnormal behavior by profiling users. With the help of algorithms to learn a user's normal behavior and establish normal user profiles based on behavioral data. He then compares user behavior against the normal profiles to identify abnormal patterns of behavior. These results will be helpful to identify abnormal behavior by monitoring user activity. Prevention, detection, counterattacking the attack to ensure and insure the safety and security of information is not only essential indispensable also. To investigate in this regard, to weigh cause and effect, and research new methods of detection, policies of prevention and counterattacking is the need of an hour.

CYBER SECURITY MEASURES

To protect private or credential information or data from outside world is necessity of every organization. Security measures include password protection, software updates, firewall, malware protections as well as authentication, authorization, auditing, reviewing, vulnerability assessment and storage encryption.

In a survey conducted by Steffani A. Burd [14] it was found that following assessment methods [Table-4] and evaluation techniques were used by the organizations to protect their sensitive information [Table-5] as a security measures.

Assessments Methods	Organizations
Vulnerability assessment	56%
Audit	51%
Risk assessment	39%
Penetration testing	36%
Application-level testing	33%
Information asset classification	25%

Table-4 – Assessment Methods Used

Evaluation Techniques	Organizations
Network traffic flow reports	75%
Help desk calls (volume/type)	74%
Firewall logs	71%
Incidents (volume/type)	64%
IDS logs	58%
Web activity monitoring software,	39%
Bot monitoring	33%
Email activity monitoring software,	31%
IPS logs	19%

Table-5 – Evaluation Techniques Used

In an organization's network, to exchange information within or outside world effectively, it is necessary to follow certain parameter or instruction. It is obligatory to give proper permissions to each of the employees or users of the network. To improve cyber security infrastructure integrity of network component like router, switch, server, work station etc we need to have security standards. Network connections need to prevent from unauthorized access. Periodic checks of its firewalls should be done to verify that the rule sets are up to the required security level. Security logs for intrusion detection systems and intrusion prevention systems can be consistently reviewed and regulated for abnormal patterns of activity. Web filter is used to protect the information being transferred from within or out of the organization. Security requirements for portable devices like USB drives, portable hard disk, IPods, mobiles, digital cameras etc that could be connected to the network. To maintain network efficiently; documentation of topology diagrams of the organization network along with geographical map showing exact location of network cables should be administered so that all the connection routes can be traced.

CONCLUSION

Throughout the literature review it has been found that by and large many organizations are not following cyber security practices. It is concluded that irrespective of the industry segment, there is a need to conduct research to find out a comprehensive approach to protect sensitive data and take appropriate action.

REFERENCES:

1. Akaninyene Walter Udoeyop, "Cyber Profiling for Insider Threat Detection", 8-2010.
2. Jeffrey R. DiBiasi, "Cyberterrorism: Cyber Prevention Vs Cyber Recovery", 12-2007.
3. Dorothy E. Denning, "An Intrusion-Detection Model", IEEE transactions on software engineering, Vol. SE-13, No. 2, February 1987, 222-232.
4. Alexandr Seleznyov, Seppo Puuronen, "Anomaly Intrusion Detection Systems: Handling Temporal Relations between Events".

5. Cory Scott, "Moving Forward", "Information Security Magazine", Volume 11-No.9, 10-2009, 32-38.
6. Douglas Jacobson, "Security Literacy - Tackling modern threats requires educating the general public about cyber security." Information Security Magazine, Volume 13-No.9, 10-2011, 23-24.
7. George V. Hulme, "SCADA Insecurity-Stuxnet put the Spotlight on critical infrastructure protection but will efforts to improve it come too late?", Information Security Magazine, Volume 13-No.1, 2-2011, 38-44.
8. Paul Marsh, "Controlling Threats", IET Computing & Control Engineering, April/May 2006, 12-17.
9. Shumba Rose, "Home Computer Security Awareness", Computer Science Department, Indiana University of Pennsylvania
10. Amitava Dutta and Kevin McCrohan, "Management's Role in Information Security in a Cyber Economy", California Management Review, Volume 45, No. 1, 2002.
11. Michael Naf and David Basin, "Two Approaches to an Information Security Laboratory", Communication Of The ACM, Volume 51, No. 12, 12/2008.
12. Power, R., "Computer Security Issues & Trends", 2002 CSI/FBI Computer Crime and Security Survey, CSI, Vol. VIII, No. 1.
13. Geer, D., Soo Hoo, K., J., Jaquith, A., "Information Security: Why the Future Belongs to Quants", IEEE Security and Privacy, 2003, pp. 32-40.
14. Steffani A. Burd, The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice, October 2006.
15. Perceptions about Network Security, Ponemon Institute, Research Report, June 2011.
16. State governments at risk: A call to secure citizen data and inspire public trust, The Deloitte-NASCIO Cybersecurity Study, 2010.
17. Robert Richardson, CSI Computer Crime & Security Survey, 2008.
18. ChiChao et al., "Cybercrime & Cybercriminals: An Overview of the Taiwan Experience", Journal of computers, Vol. 1, No. 6, September 2006.
19. Keller et al, "Information security threats and best practices in small business", Information Systems Management, Spring 2005, 22, 2, ABI/INFORM Global