2013 5th International Conference on Information and Communication Technology for the Muslim World.

Critical Information Security Challenges: An Appraisal

Mohammad Shuaib Mir[1],Sharyar Wani[2],Jamauldin Ibrahim[3]
Department of Information Systems
Kulliyah of Information & Communication Technology
International Islamic University Malaysia, Gombak 53100
mshoaib.dba@gmail.com[1],sharyarwani@gmail.com[2], jamal55@gmail.com[3]

***Abstract*— Information is one of the most crucial assets of current day organizations. However, managing this information has become a never ending challenge. Adequate security and privacy are of great essence for information systems containing valuable data and information. Leakage of such information can facilitate large-scale identity theft and successful impersonation of a victim lets the identity thief commit fraud. Identity theft occurs when someone uses another individual's personal information to pose as that individual.**

This study highlights the importance of information security management in organizations and identifies various critical security challenges that often lead to information leakage within the organizations. Qualitative method of research has been employed for data collection and analysis. The results obtained are categorized into eleven critical security challenges in order of the number of cases reported for each of them.

Keywords: Information Leakage, Security Issues, Identity Theft, Security Policy, Critical Challenges, Credentials

I. Introduction

In today's technology advanced world, information has become one of the most important resources of business organizations and managing this information has become the foremost challenge for all such organizations. It is because of this reason that security and privacy of information has become so crucial and significant for corporations all over the globe. This craving from corporations to be in command of and guard information is ingrained in the notion that information has value and is measured as the most important asset of an organization. This implies that organizations must be proficient enough to handle and administer information safely and securely. The transfer and access of organization's sensitive information, e.g. credit card details, top secrets in government agencies, personal health information etc. must be restricted within the organization's own systems and sheltered from unauthorized disclosure [1]. Before the advent of computers and internet, organizations and corporations used to store their information in secure file cabinets, however, this information is now easily and readily accessible to authorized users on computers. But the value of information to the organizations has not changed even after taking it out of the file cabinets and put on computer systems. Consequently, the security concerns also have not changed at all. Undermining this security concern of information by organizations can make them exposed to threats, which could result into huge financial losses for the companies. These threats can be categorized into five main headings as per the *UK Audit Commission (1998)* [2]:

A. *Theft* – an act of stealing data and software from an organization without authorized access.

B. *Fraud* – it is related to taking of assets by deception like making all records look consistent and normal by hiding his or her activities.

C. *Malicious Damage* –attacking an organization's system by malicious programs like viruses, Trojan horses etc.

D. *Incompetence & mistakes* – related to errors or failures by carelessness or unawareness of routine users.

E. *Accidents & disasters* - relates to destruction of computer systems due to unpredictable accidents and natural disasters.

According to a survey by Ernst & Young in 1996 with regards to loss of information due to these threats, 59 percent of companies surveyed have experienced a security breach [3]. However it does not mean that organizations and society is totally "data unsafe" as lot of efforts have been made to secure this important asset within the organizations. Nevertheless, it must not be kept in mind that this makes the situation infallible.

Due to the emergent dependence of businesses on information systems, the range and severity of threats to loss of information also increases substantially. In the past few years, corporations all over the world have changed the way they used to operate and store information. Most of the services are nowadays carried out online which help users to save time by emancipating them from the constraint of various offices' opening hours. The corporations also save resources, as users to a larger extent help themselves without talking to corporations' employees. However, these online services often manage personal information; thus making adequate security and privacy very vital for these online information systems.

Information privacy is one of the critical issues that concern an individual while dealing with the information systems. While interacting with these systems individuals have no idea of what information is available where and to whom. Information privacy is the interest an individual takes to control the flow of his personal information. Identity theft may occur when a person tries to make use of personal information

978-1-4799-0136-4/13/$31.00 ©2013 IEEE

of some other individual to act as that individual [4]. Useful information that can be leaked from information systems is e.g. name and address of a victim, credit card number and expiration dates, usernames& passwords, date-of-birth, identification numbers, results, financial information etc. This oozing of personal information can abet large-scale identity theft and successful masquerade of a victim lets the identity thief commit fraud.

Commonly known threats to an individual's privacy are dumpster diving, phishing, pharming, trojan horses, and hacking. However, there can be even major privacy concerns which are being used to maintain individual's personal information. An individual can try to protect this privacy by being careful about giving out personal information both online and offline, and keeping his operating system, firewall, and anti-virus software up to date. However, a major problem occurs as the information maintained by these corporations is beyond the individual's control, which he cannot secure [5]**.** Every year huge amounts of data leak from various systems, and governments appear to be struggling the most to keep the data safe [6] [7].

II. Related Works

Information leakage incidents have become the headlines of daily newspapers and other media. According to a CICA's white paper about data security, data breaches like laptop loss is almost about 1,000 laptops per day out of which only 3% laptops are being recovered [8]. According to [9]**,** securing data for large organizations is a big problem, as defining the contents of an information security policy as a set of security controls and to enforce them in itself is the biggest problem. Lack of security of data can also prove detrimental to large organizations by barring them from remaining competitive and having a long-term future ahead. [9] argues that an organization can be welcomed to join if it is found secure by others. This implies that suitable information protection and the testimony of it by an organization may be demanded among business partners in this epoch of electronic commerce.

Leakage of information in corporations can occur in the common ways as the corporations envisage. With regard to protecting loss of data to unauthorized parties such as external hackers, corporations nowadays invest heavily into firewalls, anti-virus software, encryptions and intrusion detection systems etc. [10]**.**The risk of information leakage also exists when organizations pool resources with other organizations and share information between each other, as the requirement for reliance on the other party's information system is not known [11]. Information leakage can sometimes also crop up from insiders of the organization as supported by a study which revealed that 87% of confidential information leaked out is from insiders [12].

According to [10] data can become more vulnerable to threats when it is easily transferred from the organization's systems to other computers by employees who use various simple portable devices (e.g. USBs, flash drives) in the work place. These devices often go overlooked as they appear risk-free to employees and become part of their normal work life. It is also argued by **[10]** that USB ports are available on every computer used today and the portable devices are simple to use and don't require any technical expertise from users to utilize them.

With the expansion of virtual networks employees can upload and store their files on an Internet accessible server and access it anywhere without being physically at their workplace. This makes data prone to leakage as employees carry data outside virtually without being noticed [10].According to a study by Cisco, 46% employees transfer organization data between their home and office with almost 75% not using any privacy screens at all[13][14].

According to [15] one of the main reasons why the organizations do not accomplish 100 percent security is the technological complexity of the organization. This complexity of technology has become a challenge for the information security experts. It is because of this complexity that the security policies formulated by the decision makers and security experts don't cover all the possible configurations of the complex systems. Various studies have been taken in the recent past to study this complexity of the technology. This includes study by [16] which focuses on the challenges posed by the complexity of wireless networks to security practitioners. The work by [17] claim that security testing of systems is a long-lasting, intricate and expensive process. The study has come-up with taxonomy to categorize vulnerabilities which will help security practitioners to prioritize resources in order to rectify these vulnerabilities.

III. Reseacrch Methodology

Qualitative method of research was employed in this study to collect and analyze data and vital information from diverse respondents. Open ended interviews, as a method of data collection, were conducted with security experts/professionals from different organizations in Malaysia and other countries. The analysis of the responses was formulated in a tabular form to identify the critical issues responsible for the information leakage issues within the organizations. Also, exhaustive exploration of books, articles and previous surveys by the research scholars as well as online resources was carried out to gain in-depth knowledge about the research topic and support the study. The results obtained were then tabulated into eleven critical security challenges that are faced by the information security professionals today according to the number of cases received for each challenge.

A. Data Collection

The data used in this study were collected by conducting open-ended interviews with security experts / system analysts system administrators from different organizations in Malaysia and other countries. The interviewees were presented with open questions about the information security and the challenges they face while dealing with information security management and notes were taken from their experiences. The questions asked were designed in such a way that they addressed the topic of the underlying research in detail. Generally the questions focused on the challenges and issues faced by the employees from time to time while they are busy in securing the information systems of their organizations.

B. Data Analysis

The information collected from the open-ended interviews was structured into key areas of focus and eleven critical issues were identified based on the number of cases reported which include unawareness of information security policy, lack of integration of systems, allowing others to use personal credentials and backing up information on the cloud among various others. These were then tabulated along with the number of cases reported from these experts for each issue. The results were derived after a careful comparison, analysis and brain storming through the tabular information and also looking at each minor issue that was taken during the interview.

IV. Findings And Results

The results based on the interviews (Table-II) conducted testify that information leakage within organizations is mainly due to eleven critical security issues which vary from unawareness of information security policies among the users to the interference from the top management of the organization.

The large amount of 244 cases reported from only 38 respondents (Table-I), shows the critical nature of the problem. It becomes quite evident that information is being leaked at a very high rate from the organizations. But the noteworthy point here is that most of the cases are taking place because of the organizational inefficiency, for example, 135 cases have been reported from C1, C2, C4, C9 and C11. These threats can be minimized to a great extent if the organization frames down a proper plan to work on them.

In this era of technology, a lot of information is being leaked and privacy seems to be a very big concern, but implementing a few steps would help in changing the scenario to a large extent. It was found that safeguarding information in its integrity and confidentiality is a really challenging task and is proving to be a never ending challenge as of now. The contribution of non-security culture was found out to be as one of the major causes for security breaches. While the practitioners want to make it sure that identity thefts are minimized, people are themselves sharing their identities which makes it tougher for practitioners.

Information security is a key concern of organizations especially when it comes to data classified as confidential and the findings show that organizations suffer from flaws from within in safeguarding this asset. The top critical challenges have been classified in the findings of this paper.

TABLE I. Response Categorization

S. No.	Organization Type	Number of Respondents
1.	Banks	**1**
2.	VOIP Service Providers	**2**
3.	Online Stores	**2**
4.	Call Centers	**4**
5.	Medical Billing Service Firms	**3**
6.	Hospitals	**2**
7.	Government	**1**
8.	University	**10**
9.	Financial Consulting Firms	**4**
10.	Telecommunication	**1**
11.	Non-profit Organizations	**5**
12.	Research Facilities	**3**
	Total Number of Respondents	**38**

TABLE-II. Security Issues and Cases

	Critical Security Issues	No. of cases reported
C1.	Unawareness of information security policy	**35**
C2.	Lack of integration of systems	**26**
C3.	Allowing others to use personal credentials	**8**
C4.	Backing information on the cloud	**42**
C5.	Accessing websites whereby threats are downloaded	**37**
C6.	Unauthorized file sharing	**18**
C7.	Seldom policy following about information security	**15**
C8.	Password Sharing	**23**
C9.	Lack of efficient internal backup system	**12**
C10.	Inefficient knowledge sharing between departments	**8**
C11.	Top management interferences	**20**

V. Discussion

The results obtained from the interviews were categorized mainly into eleven top critical security issues neglecting others based on the minimal number of cases reported for them. The different security challenges seem to be very critical as per the number of cases reported as depicted in Table II. It was observed that the most information leakage cases were reported because of transfer of information to the cloud for the backup purposes. This takes place because of the fact that most organizations do not have proper and efficient backup systems in place. It was also found that top management interference can be devastating for an organization because the security expert has to compromise sometimes, which in turn may be a cause for many of the above reported information security challenges.

Open access to websites whereby the computers can get infected by malware, etc stands out to be the third in its order of critical nature. The problem with the access to these websites is not only that it affects the computer and decreases its performance but stuff like Trojans can send out important information such as credentials into the cloud which can be a major source of breach of security, thus leading to information leakage.

It is noteworthy to observe that the cases reported due to unawareness about the Information Security Policy of the organization stand third right next to Accessing websites whereby threats are downloaded. This simply implies that employees are not introduced to security policies of the organization and in cases where they are introduced to them; policies seem to be so weak that the employees hardly get affected by it. Even if a breach occurs, there is no proper and strict clause for action against the organization members or more specifically speaking leakage of information.

It is worth to mention here that proper integrated systems would lead to a proper knowledge sharing environment which would help to reduce the risks to a large extent. It was striking to find that Integration of systems which is not thought of as a challenge in the information security world as per the available literature –is a major challenge in the real world as is evident from the Table-II with number of cases being reported 26.

There arises a need to address these security challenges as enormous amount of information is being leaked out though high claims are being made about security and privacy. The need for implementing security measures is inevitably desirable right away as a lot of information is being leaked out. In reality privacy seems a big concern though lot of discussions is being done on safeguarding of privacy and data. The challenges need to be addressed as soon as possible. A lot of academic work has been published and discussions are being made consistently regarding this issue. At the same time numerous sophisticated tools have been designed but the reality is that a couple of steps can help to minimize the challenges which in turn will help to reduce the threats that are being faced in the information security world. The fact is that information leakage can be brought to a minimum.

VI. Conclusion

In this study, importance of information security management for organizations has been highlighted and top critical challenges to information leakage were highlighted. The work used qualitative approach to identify the top critical challenges in information security management with regard to information leakage. The analysis of the data collected was carried out and results obtained were categorized into eleven critical security challenges in order of the number of cases reported for each of them.

References

[1] Imad M. A, Muntaha A (2008), Preventing Insider Information Leakage forEnterprises, The Second International Conference on Emerging Security Information, Systems and Technologies.

[2] http://www.legislation.gov.uk/ukpga/1998/18/contents. Retrieved on 05 November, 2012.

[3] Bocij, P.; Chaffey, D.; Greasley, A. and Hickie, S. (1999) p:538 "Business Information Systems: Technology, Development and Management." Financial Times Management, London.

[4] S. T. Kent and L. I. Millett, editors, Who Goes There? Authentication through the Lens of Privacy, The National Academies Press, 2003.

[5] B. Schneier, "Risks of Third-Party Data," Communications of the ACM, 48(5):p. 136, May 2005.

[6] Privacy Rights Clearinghouse, "A Chronology of Data Breaches," http://www. privacyrights.org/ar/ ChronDataBreaches.htm, last checked Feb. 14, 2008.

[7] Symantec Inc., "Symantec Internet Security Threat Report XI," March 2007.

[8] Trites, Gerald D. "Data-Centric Security – White paper from CICA."

[9] Von Solms, S.H. "Information Security and Electronic Commerce" Proceedings of IFIP/Sec98, Budapest, Hongarye, 1998.

[10] Mallery, J. (2009). Overlooked Data Leaks. Security Technology Executive , Volume 19(3), p:78-80, 82.

[11] Alawneh, M. Abbadi. (2008). Preventing Information Leakage between Collaborating Organizations. Proceedings of the 10th International Conference on Electronic Commerce (pp. 1-10).

[12] Baek, E. K. (2008). The Design of Framework for Detecting an Insider's Leak of Confidential Information. Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, information, and Multimedia and Workshop, (pp. 1-4).

[13] Data Leakage Worldwide: Common Risks and Mistakes Employees Make - A white paper from Cisco. Retrieved on 05 November 2012.

[14] Data Leakage Worldwide: The High Cost of Insider Threats – A white paper from Cisco. Retrieved on 05 November 2012.

[15] Audestad, J. (2005), "Four reasons why 100% security cannot be achieved", Telektronikk, Vol. 1,pp. 38-47.

[16] Welch, D. and Lathrop, S. (2003), "Wireless security threat taxonomy", paper presented at:Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, pp. 76-83.

[17] Jiwnani, K. and Zelkowitz, M. (2002), "Maintaining software with a security perspective",Proceedings of the International Conference on Software Maintenance, pp. 194-203.

[18] Mikko T. Siponen, (2000),"A conceptual foundation for organizational information security awareness", Information Management & Computer Security, Vol. 8 Iss: 1 pp. 31 – 41, Emerald.

[19] Dinesha H A, Agrawal V K, Multi-level Authentication Technique for Accessing Cloud Services, " Computing, Communication andApplications (ICCCA), 2012 International Conference on , vol., no.,pp.1-4,22-24,Feb.2012doi:10.1109/ICCCA.2012.6179130, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6179130&isnumber=6179125.