Information Security Risks Awareness Based on Categories

Syed Raza
Trenholm State Technical College
sraza@trenholmstate.edu

Abstract

Almost 80% of computer users are affected by some type of security threat due to unawareness about security. Different studies show that it is understood that most businesses do not receive enough information security consulting from within and/or outside the organization. In addition, it was found that most businesses are not sufficiently involved in information security standards to be able to implement them in their organizations. Billions of dollars are spent yearly on computer security because it ranks as the world's number one concern. It has also been reported that awareness of information security is the fundamental key in understanding various information security threats and in perceiving vulnerability related to these threats. The increasing utilization of information technology is affecting the status of information security and is gradually becoming an area that plays an important role in everyday life. The term "information security" is more commonly used to describe the tasks of protecting information in a digital format. Information security threats are events and actions that present a danger to information assets. Information security is included in organizations, the public, sociopolitical, computer ethical and institutional educational dimensions. For this reason, information security should be taken very seriously; the rules should be read and followed. This project involves the collection of various risk factors that could result in great losses to businesses, industries, institutions, and their employees if information is breached. The focus of this research was based on prior literature reviews identifying the factors that contributed to security risk of industries, educational institutions, and employees. The research has developed the security awareness risk model (SARM), which includes the risks as well as losses and outcomes

Introduction

Security's role is much more important today than it was years ago. Billions of dollars are spent yearly on computer security because it ranks as the world's number one concern. Although bundles of money are spent on security, the number of attacks is continuing to increase. It has been reported that the lack of compliance with an information security policy is due to unavailability of the policy [1, 8]. It has also been reported that awareness of information security is the fundamental key in understanding various information security threats and in perceiving vulnerability related to these threats. However, an understanding of threats alone seems not to be enough to motivate action [2, 9].

Information security is a critical issue that many firms currently face; while increasing incidents of information security breaches have generated extensive publicity, previous studies repeatedly expose low levels of managerial awareness and commitment, a key obstacle to achieving a good information security posture. In fact, it has been reported that a

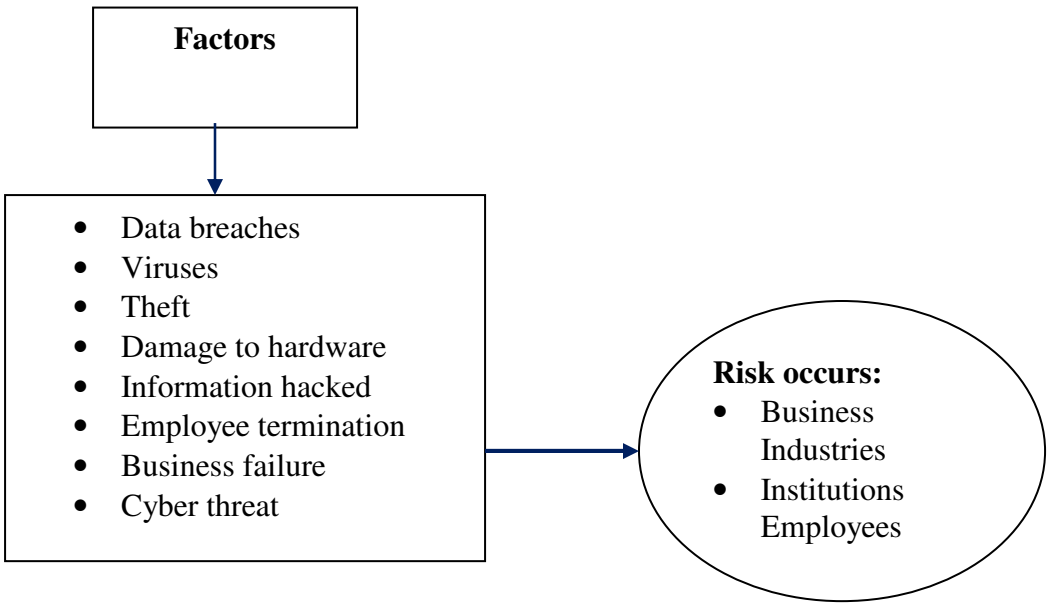
reason why information system security incidents and abuses continue to plague organizations is that employees are the weakest link in ensuring information systems security: they constitute an insider threat to their organizations [3, 10].

Computer users should be aware of the risk factors involved in security and should be knowledgeable of the steps that can be taken to reduce risk of becoming a victim to security breaches. Receiving or sending incorrect data could result in security problems such as system crashes that can severely damage or erase valuable data. Fraud and theft are two common risk factors and can be highly undetectable. It is important to use passwords and security codes to ensure that those who have access to certain information have permission are trustworthy. Viruses, worms, and trojan horses are malicious codes, uninvited software that can damage information. It is vital to maintain certain spyware and security protection software to limit the chance that information will fall prey to this type of program. Employees are still involved in risky behaviors that put businesses at risk, despite the security policies, standards, awareness strategies, and tools currently in place. Security-related behavior in the workplace has recently been a major focus in the information systems literature [4, 11].

Positive and negative security-related behavior in the workplace is a big focus in information systems literature. Studies reported security-related behavior to be inconsistent and sometimes contradictory results about the effects of some factors such as sanctions [5]. Employees violate policies, creating threats to businesses or organizations due to unawareness. Some threats are created intentionally and some unintentionally. This research has developed the security awareness risk model (SARM) to identify the factors that provoke security risks and losses for businesses, industries, educational institutions, and employees.

Security Awareness Risk Model (SARM)

The focus of this research was based on prior literature reviews identifying the factors that contributed to security risk of industries, educational institutions, and their employees on the basis of the risk model, presented in Figure 1. Several factors associated with security have been reported in different studies. These factors were implemented in the literature review on protecting information in the digital format involving losses and outcomes. The security awareness risk table includes the risks as well as losses and outcomes, as shown in the results section.



Result

All these factors are based on the categories and associated risk or threats are linked with losses of personal information that may damage the infrastructure of industries and reputation of institutions. Even though information collected on industries, educational institutions, and their personnel is protected by the United States Information Security and Federal Information Security and Data Breach Notification Laws, this information may be breached [6, 7].

Table 1. Security awareness risk matrix

Category	**Reported Factors**	**Risk/Threat**	**Losses/ Outcomes**	**Prior Literature**
Lack of awareness	-Employees causing problems to businesses -Cybercrime attempts	-Employees could be terminated -Businesses could fail -Data breaches -Personal information could hacked	-Businesses will become victim -Revenue compromised -Spending increase -Security failure -Drive repair -Head crashes	[2, 12, 13]
Security-related behavior	-Policy violation -Computer abuse	-Viruses -theft -Damage to hardware	-Profits are compromised -May be sued -Student enrollment decline	[5, 10]
Lack of compliance	-Security rule compliance are not being met -Failure to change passwords -failure to update security patches -failure to backup	-Information could be hacked -Employees could be terminated -Businesses could fail	-Decreasing of employees and well as the business	[1, 3]

Table 2. Security awareness risk matrix: categories

• Lack of awareness: - vulnerable to "cyberattacks" and malicious information technology (IT) - vulnerable to "cyberthreats" - loss of revenue - facilitate exploitation, revenge, economic, political, or social harm and disruption - damage to IT assets - possible perpetrators of malicious IT recovery costs - related cost of avoidance cyber attacks • Lack of compliance: - individual responsibilities
- facilitate exploitation, revenge, economic, political, or social harm and disruption - damage to IT assets - possible perpetrators of malicious IT recovery costs - related cost of avoidance cyber attacks • Security related behavior: - avoidance behavior - safeguard resources - facilitate exploitation, revenge, economic, political, or social harm and disruption - damage to IT assets - possible perpetrators of malicious IT recovery costs - related cost of avoidance cyber attacks

Recommendations

Most of the discussion in the literature focuses on the prevention techniques by using technical countermeasures; therefore, organizations should optimize their limited resources. This paper has investigated various risk factors due to noncompliance standards of security, unawareness of the policies, and ignorance of business security risks.

In future work, how security strategies are developed and utilized in organization will be explored. Therefore, personal interviews and surveys will be conducted to validate the various risk factors that could result in great losses for those areas indicated in Table 1. All participants in the focus groups will be related to the positions such as security manager, IT manager, security consultant, security research, and development director, and they will be required to have more than four years of experience. Moreover, detailed recommendation will be shared with them after compiling the data to improve awareness of security risk and increase the usage of security mechanisms in the organization.

Conclusion

Privacy policy information is a priority and policies are constantly being upgraded and revised in order to maintain confidence and trust. Protecting computerized information is a major concern and reality today. This project involved the collection of various risk factors that could result in great losses for those areas indicated in Table 1. One is not always aware of how this information can be violated and the resulting ripple effects that can occur. All parties and entities involved should become aware of, engage in secure behavior, and comply with secure policies. These steps are taken to safeguard and avoid misuse, abuse, and destruction of computer digitized information. More educational security awareness programs should be introduced. It should be included in everyday practices, thereby resulting in a greater compliance with security rules. Due to the seriousness and sensitivity of information security, it is very important that industries, institutions, and employees understand and comply with all security policies, provide a safer and securer working environment by implementing their own SARM.

References

[1] Kolkowska, E. & Dhilllon, G. (2013, March). Organizational Power and Information Security Rule Compliance. *Computers & Security*, *93*, 3-11.

[2] Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic Optimism on Information Security Management. *Computers & Security*, *31*(2), 222-232.

[3] Infinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, *31*(1), 83-95.

[4] Hashimoto, G., Rosa P. F., Filho, E. L., & Machado, J. T. (2010). Security Framework to Protect against Social Networks Services Threats. *Fifth International Conference on Systens abd Networks Communications*, 189-193.

[5] Guo, K. (2013, February). Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. *Computers & Security*, *32*, 242-251.

[6] Leahy, S. (2011). *Personal Data Privacy and Security Act*. Retrieved from http://www.leahy.senate.gov/imo/media/doc/BillTextPersonalDataPrivacyAndSecurityAct.pdf

[7] Congressional Research Service (CRS). (2012, April 10). *CRS Report for Congress 7-5700, R42475*. Retrieved from http://www.crs.gov

[8] Fuchs, L., Pernul, G., & Sandhu, R. (2011, November). Roles in Information Security —A Survey and Classification of the Research Area. *Computers & Security*, *30*(8), 748-769.

[9] Mejias, R. (2012, January). An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. *45th Hawaii International Conference on System Science*, 3258-3567.

[10] Qian, Y., Fang, Y., & Gonzalez, J. J. (2012, November). Managing Information Security Risks during New Technology Adoption. *Computers & Security*, *31*(8), 860-869.

[11] Ciampa, M. (2010). Introduction to Security. In *Security Awareness: Applying Practical Security in Your World* (1-36). Boston: Course Technology.
[12] Takemura, T. (2011, October). Empirical Analysis of Behavior on Information Security. *International Conference on and 4th International Conference on Cyber, Physical and Social Computing, Internet of Things*, 358-363.
[13] Yildirim, E., Akalp, G., Aytac, S. & Bayram, N. (2011, August). Factors Influencing Information Security Management in Small and Medium-Sized Enterprises: A Case Study from Turkey. *International Journal of Information Management*, *31*(4), 360-365.

Biography

SYED RAZA is currently a Computer Information Systems instructor at Trenholm State Technical College. Recently, he completed his leadership montgomery training. During his training, he was involved in different community services and addressed the issues in higher education and business industries. Also, he has also over 15 years of experience as an educator and software engineer. Dr. Raza may be reached at sraza@trenholmstate.edu.