Good recommended technologies processes and policies for insider theft of intelle...

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Information Security White Paper

Abstract

The growing use of computer systems and networking in the business world has resulted in an increase in information security threats. Perpetrators have developed malicious codes and spyware, which they use to gain information from business normally for financial gain. Most of the threats and vulnerabilities that are experienced may emanate from unintentional or intentional attacks. Mitigations applied to the threats depend on the threats, and it is necessary for risk assessments to be carried out to ensure appropriate technologies, processes and policies are set up to ensure information security is not compromised. Failure to have an information security system may result in additional cost implications that are normally associated with a cost of notifying clients in the event of a breach of data in a business and loss of clientele.

Business need for information security

The current advancement in information technology has brought about much positive change in the business environment. This change is in terms of how transactions and different processes are done in businesses. However, such changes in information technology has brought about negative aspects, which mainly rests on the increasing need to protect business information from malicious individuals that seek to exploit vulnerabilities in various information technology systems applied to the different businesses. According to Whitman and Mattord (2012), attacks on information systems have become a daily occurrence. Information security in a business is important for several different reasons. According to Whitman and Mattord (2012), one of the important reasons for implementing an information security system in a business is to protect the data and information an organization collects and uses. Secondly, an information security program or system aims to ensure that the information technology applications run safely without disrupting the business processes of the organization and at the same time ensure the business assets are protected. Kissel (2009) notes that for small businesses, information security is important as the customers expect their sensitive information to be respected and provided with adequate protection. Furthermore, other business partners need assurance that any transactions with the small businesses will not result or put their systems at risks. As such, most business partners require business they transact with have a similar level of security as their systems (Kissel, 2009). Information that needs to be protected can vary from financial information, health information or privacy information. Failure to protect, appropriately,

such information may result in fines and penalties that are administered by certain regulatory agencies (Kissel, 2009). Failure to protect information may cause a business to incur additional costs such as those incurred in notifying clients or customers that there is an occurrence of a security breach, and their information has been compromised. In such cases the more the number of clients the higher the cost of notification (Kissel, 2009).

Information Security threats and Vulnerabilities

Threats and vulnerabilities to information security are closely linked. Threats normally exploit vulnerabilities in an information security system. Threats to any business information system can be intentional or unintentional. According to Wilshusen (2009), unintentional threats normally emanate from untrained employees, failure to perform relevant software upgrades or maintenance procedures that may corrupt data. Intentional threats are those that have a sole purpose or goal to steal or compromise a business information system.

One of the common threats to many information systems is viruses. According to Dhotre and Bagad (2009), a virus is a malicious code that is designed to infect other programs by modifying them. Viruses are normally designed to spread from one computer to another. According to Erbschloe (2004), viruses' main aim is to corrupt files in an organization's system and eventually disable the computer security software to allow further attacks on the system. Viruses fall under the class of malicious software that may include worms and Trojan horse. Worms normally feature as standalone applications whereas Trojan horses are normally attached to a program prior

to its distribution (Dhotre and Bagad, 2009).

Spyware is another form of threat to information systems. According to Erbschloe (2004), spyware are used to gather information about an organization or client information in a certain organization. As such, spyware can gather information such as keystrokes of passwords and bank account details that are installed in a computer. Such collected information can be used for personal reasons or are profit motivated where they are sold to third parties.

In understanding the various aspects of threats and vulnerabilities, it becomes important to have an idea what some of the key concepts in information security stand for. According to Whitman and Mattord (2013), a key concept in information security is confidentiality. This implies that access to information is only allowed to those who have the necessary privileges to that information. Any access to information by unauthorized individual implies that confidentiality is breached. Even within the same organization, different individuals will have different levels of privileges when it comes to confidential matters. Integrity as a concept of information security relates to the status of information, which is not exposed to damage, corruption or disruption from its genuine state (Whitman and Mattord, 2013). Viruses and worms are designed to compromise the integrity of data by corrupting it. According to Whitman and Mattord (2013), availability is another concept of information security, which relates to the usability of information without any form of obstruction. It is important to note that availability, in this case, implies that information is usable by the authorized personnel. As such, the formats of data need to be in a usable form to the authorized personnel.

Access to the information system requires authentication, which refers to the process where a control ascertains whether a user, has the identity they state to have (Whitman and Mattord, 2013). Common forms of authentication that are mostly used involve personal identification numbers or passwords, which authenticate the user's identity to the system. Authorization is the process that follows authentication. Through authorization, a system ascertains the level of access a user has to access and modify different information in the system (Whitman and Mattord, 2013). A user may be authorized only to input data while another may be authorized to transfer data to different systems (Whitman and Mattord, 2013). According to Wheeler (2011), nonrepudiation is a form of assurance that exists through digital signatures as a proof of the sender's identity and proof of delivery of data to the recipient. Risk relates to the likelihood that some undesired event such as denial of service attack or information corruption could cause financial losses (Raggad, 2010).

One common method employed in insider theft of intellectual property involves the use of removable media. According to Cappelli, Moore and Trzeciak (2012) any access to removable media needs to be restricted to only specific users that have certain roles within the business information system. Policies that establish the use of removable media in the system need to be setup. If a user intends to use removable media, specified protocols need to be authorized to ensure that the media is not used for other purposes other than the task required. Company owned media should not be allowed to leave the facility or the business premises. Emails sent to

competitors through the company’s information network need to be monitored more closely to ensure that sensitive information is not being transferred or shared (Cappelli, Moore and Trzeciak, 2012).

Impacts that can be expected

Investing in security by a business helps it reduce the occurrence and severity of information security related losses (Van, 2008). Kissel (2009) notes additional costs can be incurred in situations where the business fails to protect customers’ information. Depending on the states notifications laws for all businesses, customers are required to be notified of any security breach, such notifications may cost an organization about $100 per customer. As such, if the organization has a huge client base the cost of notifications is high. Furthermore, another cost incurred in situations where a business security is compromised is that clients will take their business to organizations that seem more secure.

References

Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Upper Saddle River, NJ: Addison-Wesley.

Dhotre, I., & Bagad, V. (2009). Information Security. Pune: Technical Publications.

Erbschloe, M. (2004). Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code. Burlington: Elsevier.

Kissel, R., & National Institute of Standards and Technology (U. S.). (2009). Small business information security: The fundamentals. Gaithersburg, Md.: U.

S. Dept. of Commerce, National Institute of Standards and Technology.

Raggad, B. (2010). Information Security Management Concepts and Practice. Hoboken: CRC Press.

Van, S. C. (2008). Information communication technologies: Concepts, methodologies, tools, and applications. Hershey, Pa: Information Science Reference.

Wilshusen, G. (2009). Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk: Congressional Testimony. DIANE Publishing.

Wheeler, E. (2011). Security risk management: Building an information security risk management program from the ground up. Waltham, MA: Syngress.

Whitman, M. E., & Mattord, H. J. (2012). Principles of information security. Boston, MA: Course Technology.

Whitman, M. E., & Mattord, H. J. (2013). Management of information security.