Information Security White Paper

Introduction

Information security is an essential part not only for large businesses but also for small ones. Many small businesses do not have the information security strategy, and they do not care about it until an emergency happens. Security breaches can have dangerous consequences for the company such as decrease of productivity, customer loyalty, the ability to compete, and even the loss of entire business. Therefore, information security is an essential part of any business that serves to protect personal information from security breaches.

Protection Measures

Many experts believe that information is always at risk no matter how well the business is protected (Porter, 2009). The threat that is growing every day can be devastating, and every business needs information technology security strategy to protect the property, employees, and products. Security managers understand the growing threat of technology, and they improve protection measures by locking the doors, hiring trusted employees, and so on. Not to get into trouble with security threats, small businesses should pay attention to cyber-crimes. Outsourcing can protect business from potential risks, but it is important for small businesses to realize threats and provide security measures that can medicate these threats. Businesses could not just rely on outsourcing solutions, but they should also obtain specific knowledge about possible threats and their consequences.

The research asserts that small businesses should collaborate with FBI to receive the information concerning possible threats on the local and national levels (Whitman & Mattord, 2010). In order to protect information, employees should obtain special training and education accompanied by practical assistance. Business owners should learn how to secure information and make the right investments defining their security needs and potential threats. They should also stay current and learn the best world practices.

Information Security Threats and Vulnerabilities

Smith (2013) assumes that there are four major types of cyber predators such as hacktivists, cyber criminals, information warriors, and experimenters or vandals. Hacktivists manipulate in accordance with the political or personal agenda while cyber criminals do it because of money. Information warriors work professionally in a national level aiming to disrupt whole systems. Experimenters and vandals are non-professional attackers who commit cyber-crimes to improve their reputation for themselves. However, cyber threats do not just come from outside, they can also exist inside the organization. Insider threats are the result of the 80 percent of the attacks to small businesses (Whitman & Mattord, 2010). No matter where the threat is coming from it has the same aim: access to business information. Therefore, business owners should protect their companies from loss of profits, costs of litigation and spoiled reputation.

Theft of data and resources can be easy to rich for cyber attackers because employers and employees use digital devices did not realizing that the information can have an easy access to others. Denial-of-service attacks are another information security threat that is used to blackmail the business. They demonstrate that if the owner did not pay them they could disrupt the business. Attackers can install malicious code on a system and damage programs by silently watching what is going on in the business. Viruses that present about 70 kinds of them make a kind of malicious code. All these threats can destroy or damage an average small business. Vacca (2012) asserts that information security threats and vulnerabilities of small businesses can pose a threat to the whole nation.

Key Concepts as Part of the Threats

In order to maintain information security, it is important to understand some key concepts like a part of the threats and vulnerabilities. Smith (2013) believes that confidentiality can be a part of cyber security measures, and the data cannot be modified by users. Integrity requires the consistency and accuracy of data in the business process and

protects it from unauthorized use. Availability is also at the core attention of information security because information systems should be available at all times for those who need them. Non-repudiation offers actions that protect information security such as introducing a key card that gives the permission to assess the system. This card could not be shared with other employees, and one should immediately report in case of its theft. An individual should not give access to others to use his or her computer, or giving others personal password denying owners from denying actions. Authentication is the process that confirms the identity of a person by checking his or her documents, verifying various information and compliance with the original data. Authorization gives the right of access to the informational resources that maintains control of them. It is based on access policy that allows users to enter the computer system and use individual files, programs, data, and computer devices. Risk is a threat that something bad may happen and damage an information asset.

Recommendations

Many experts consider that all these steps can help organizations and personal users to improve their informational security and protect them from potential risks (Maddock, 2010). There are different technologies, processes, and policies that can be used by senior leadership in HR, data owners, legal, and information security to solve or mitigate insider theft of intellectual property. It would be reasonable to check insiders' email, printed documents, removable media, file transfer, and laptops where they can download sensitive files. Insiders remove information through data exfiltration, and managers should track or even block their email to and from competitors. The business owners should also check for large email attachments to different email accounts. Monitoring and control of all files should be thoroughly provided in an organization. All these protective actions should be considered in making contracts.

Conclusion

Small businesses must realize that they can be vulnerable to security breaches as well as large businesses. To protect private information, business owners should develop information security strategy and inform all employees about it. The ever-changing technology creates more security threat to information, and the staff should be well-trained to take appropriate measures to prevent possible threats. Business owners of small enterprises should realize that limited knowledge of computers, software, and networks give an easy access to cyber criminals and computer hackers.