Investing in IT Security: How to Determine the Maximum Threshold

Amanda Eisenga, Lutgert College of Business, Florida Gulf Coast University, USA
Travis L. Jones, Lutgert College of Business, Florida Gulf Coast University, USA
Walter Rodriguez, Lutgert College of Business, Florida Gulf Coast University, USA

ABSTRACT

Investing in information technology (IT) security is a critical decision in the digital age. And, in most organizations, it is wise to allocate a significant amount of resources to IT infrastructure. However, it is difficult to determine how much to invest in IT as well as quantifying the maximum threshold where the rate of return of this investment is diminishing. The main research question in this paper is: how much and what financial resources should be allocated to IT security? This paper analyzes different practices and techniques used to determine the calculation for investments in IT security and analyzes and recommend some suitable methods for deciding how much should be invested in IT security.

Keywords: Information Technology, Information Technology Security, Investing in Information Technology, Maximum Threshold, Security Methods for Information Technology

INTRODUCTION

Investment in IT security is an important aspect in any business to help mitigate the risk of security breaches and challenges, such as, an attack or a negligent employee. These challenges can be internal with the use of intruders or external with the use of hackers. Further, a negligent employee can cause a risk to a company by exposing data and not taking the precautionary steps to avoid a security breach. These types of security breaches are discussed. Security breaches cost companies on average $214 per compromised record breach for 2010 (Ponemon Institute LLC and Symantec, 2010). In 2011, the average per compromised record breach for 2011 decreased to $194 (Olavsrd, 2012). The decline was a result from a decline in lost business costs: abnormal turnover of customers, increased customer acquisition costs, reputation losses and diminished goodwill (Olavsrd, 2012) (Figure 1).

The average organizational cost of a data breach was $5.5 million in 2011 (Olavsrd, 2012). In 2010 and 2011, the Ponemon Study found that negligence caused 39% of the data breaches. Insiders in the organizations still pose a serious threat for an organization especially with the increase in adopting the use of tablets smart phones, and cloud application (Olavsrd, 2012). With the new technology, employees are able to access an organization’s information anywhere and anytime (Olavsrd, 2012). Data breaches compromise any corporation’s reputa-
Companies must invest in IT security, so they are protected from intruders, hackers, viruses and malwares, which could cause data breaches. A data breach occurs when intruders gain access to the company’s IT infrastructure. These intruders can gain access through easy passwords or employees divulging privileged information. This allows the intruder to create havoc. The intruder can add or delete information, alter programs, or even create “time bombs.” Time bombs are created with the use of a code and are scheduled to “explode” unexpectedly, creating a disaster.

Hackers are external and try to disrupt the system with attacks. An attack can be performed as a denial of service (DoS). A DoS attack occurs when the infrastructure device is disabled by flooding the servers with too many messages. This overwhelms the system, and every message appears to be an authentic interaction. A distributed denial of service (DDoS) occurs where an attack is initiated from multiple sources instead of a single source (Applegate, Austin, & Soule, 2009).

Viruses and malwares threaten a company’s infrastructure. These are software programs that replicate and spread themselves throughout computers. The damage can be minor but also can incorporate and automate other attacks, such as a DoS attack.

Negligence by an employee is an unintentional compromise of the server or information. An example of this is if an employee is speaking loudly about a new project or if an employee’s work laptop is stolen. This exposes the company to risk. A negligent employee may not be receiving the right education tools to know how to protect the company. Even if the employee has received the right training, the employee may not be implementing the steps to protect his employer.

**COST OF EXPOSURE TO A SECURITY BREACH**

A security breach heavily affects a company, which is why a company has to invest in some type of security, if only a minimal investment. If a company does not invest in IT security, the company will be 100% exposed to a security breach. The costs of security breaches are composed of loss of productivity, reputation, customer perception, and recovery of expenses.

The cost of loss of productivity is not easily determinable. Productivity loss will include how much service the company has lost and employees not being able to do their job properly, because the IT system is down. Loss of productivity, and therefore its cost, increases with how long the IT system is down (Sonnenreich, Albanese, & Stout, 2006). If the company’s IT system is down for two to four days, this will significantly affect the company. For example, suppose a company that is solely based online, and mainly makes its revenue during the winter holidays, has a

---

Figure 1. Average investment cost from 2005 to 2011
Related Content

Network Intrusion Detection and Prevention Systems on Flooding and Worm Attacks
www.igi-global.com/chapter/network-intrusion-detection-and-prevention-systems-on-flooding-and-worm-attacks/156460?camid=4v1a
Formulating a Code of Cyberethics for a Municipality
[www.igi-global.com/chapter/formulating-code-cyberethics-municipality/13488?camid=4v1a](www.igi-global.com/chapter/formulating-code-cyberethics-municipality/13488?camid=4v1a)

Cost Estimation and Security Investment of Security Projects
[www.igi-global.com/chapter/cost-estimation-and-security-investment-of-security-projects/213649?camid=4v1a](www.igi-global.com/chapter/cost-estimation-and-security-investment-of-security-projects/213649?camid=4v1a)

Extending Security in Agile Software Development Methods
[www.igi-global.com/chapter/extending-security-agile-software-development/24054?camid=4v1a](www.igi-global.com/chapter/extending-security-agile-software-development/24054?camid=4v1a)