Available online at www.sciencedirect.com
ScienceDirect
International Journal of Information Management 28 (2008) 413–422
International Journal of Information Management
www.elsevier.com/locate/ijinfomgt

An economic modelling approach to information security risk management

Rok Bojanc, Borka Jerman-Blažič*

Faculty of Economics, Ljubljana University and Jožef Stefan Institute, Jamova 39, Ljubljana, Slovenia

Abstract

This paper presents an approach enabling economic modelling of information security risk management in contemporaneous businesses and other organizations. In the world of permanent cyber attacks to ICT systems, risk management is becoming a crucial task for minimization of the potential risks that can endeavor their operation. The prevention of the heavy losses that may happen due to cyber attacks and other information system failures in an organization is usually associated with continuous investment in different security measures and purchase of data protection systems. With the rise of the potential risks the investment in security services and data protection is growing and is becoming a serious economic issue to many organizations and enterprises. This paper analyzes several approaches enabling assessment of the necessary investment in security technology from the economic point of view. The paper introduces methods for identification of the assets, the threats, the vulnerabilities of the ICT systems and proposes a procedure that enables selection of the optimal investment of the necessary security technology based on the quantification of the values of the protected systems. The possibility of using the approach for an external insurance based on the quantified risk analyses is also provided.
© 2008 Elsevier Ltd. All rights reserved.

Keywords: ICT security tools; Risk management; Technology investment

1. Introduction

The Internet evolution is one of the greatest innovations of the twentieth century and has changed lives of individuals and business organizations. Sharing of information, e-commerce and unified communication are some typical main benefits of using the Internet. Trends like globalization, higher productivity and reducing the costs make business organizations increasingly dependent on their information systems and the Internet services. Potential attacks on the information systems and eventual crash may cause heavy losses on data, services and business operation. Security risks are present in the organization's information system due to technical failures, system vulnerabilities, human failures, fraud or external events. This is the main reason why organizations are investing in information security systems, which are designed to protect the confidentiality, integrity and availability of information assets. Due to the rising awareness regarding the potential risks of attacks and breaches, the investments in information security are increasing and are taking different approaches depending on the area of applications. Although security technologies have made great progress in the last 10 years, the security level of computers and networks has never been considerably improved (Schneier, 2004; Whitman, 2003).

Almost a decade ago, a number of researchers began to realize that information security is not a problem that only technology can solve and tried to include also an economic point of view. This approach enables business managers' better understanding of security investments, because the importance of security failure is presented through economical losses instead of technical analysis. This is the reason why security-aware organizations are shifting the focus on the prevention of possible failures from what is technically possible to what is economically optimal (Anderson, 2001; Anderson & Schneier, 2005; Schneier, 2004).

*Corresponding author. Tel.: +386 41 678 410; fax: +386 1 477 3395.
E-mail addresses: rok@bojanc.com (R. Bojanc), borka@e5.ijs.si (B. Jerman-Blažič).

0268-4012/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2008.02.002

When looking on information security system from economics point of view, economics can actually provide answers to many questions where just technical explanation has no satisfying answer: how does an organization become secure in its IT-based operation? Which security level is adequate? How much money should be invested in security? Business organizations try to solve these questions in terms of risk management.

Information security risk management is the overall process which integrates the identification and analysis of risks to which the organization is exposed, the assessment of potential impacts on the business, and deciding what action can be taken to eliminate or reduce risk to acceptable level (NIST, 2002). It requires a comprehensive identification and evaluation of the organization's information assets, consequences of security incidents, likelihoods of successful attack to the ICT systems, and business costs and benefits of security investments (Hoo, 2000). Standards and guidelines are available for information security management, such as the ISO 27000 series and NIST publications (ISO, 2005; NIST, 2008). Security risk management applied by an organization usually consists of:

1. identification of the business assets;
2. threats identification and damage assessment that may be caused by successful attack;
3. security vulnerabilities of the systems that the attack may exploit;
4. security risk assessment;
5. measures to minimize the risk with implementation of appropriate controls;
6. monitoring the effectiveness of implemented controls.

This paper proposes a standard approach towards assessment of the required ICT security investment and data protection. In the approach proposed, the assets, the threats and the vulnerabilities of the ICT systems are identified first through a security risk analysis; then a method for quantification of the necessary investment in security provision is described. The paper ends with discussion of the applicability of the approach for enterprise security risk, an external insurance based on the quantified risk analyses.

2. Gathering the data for security risk analysis

The goal of security risk analysis is to identify and measure the risks in order to inform the decision-making process. Risk analysis needs the data about information assets in the organization, threats to which assets are exposed, system vulnerabilities that threats may exploit and implemented security controls.

2.1. Identifying the assets and their value for the organization

The first step in security risk analysis process is to identify the organization's information assets. Assets are information and resources that have value to the organization. After the asset is identified it must be evaluated. The valuation of tangible assets is pretty easy; they are measured in money, with depreciation taken into account. Tangible assets include physical infrastructure (such as servers, workstations and network infrastructure) and software elements of the information system. Usually, the valuation of intangible assets such as business data, organization knowledge, company reputation and the intellectual property stored within the organizational system is more difficult.

When the assets are assessed they are usually classified into discrete categories, or class (FIPS, 2004; Microsoft, 2004; NIST, 2004). The classes facilitate the definition of the overall security risks. They also help the organization to focus on the most critical assets first. Different risk assessment models define a variety of asset classes. While a larger number of classes (e.g. 10) is more precise, a smaller number (e.g. 3 or 4) of classes reduces the time to debate and select the appropriate class designation. An example of a three-class model is critical, moderate and low-asset class. Typical critical assets are financial data, intellectual property, bank account numbers, etc. Among moderate assets are internal business information, purchase order data, network designs and information on internal web sites. Low-asset class typically presents information on publicly accessible web pages, published press releases, product brochures and white papers.

2.2. Identifying the threats

An organization's information assets are exposed to threats. A threat is any potential event with an undesirable impact. To strengthen the level of protection and establishment of security strategies, organizations must clearly identify the threats facing their information assets.

The common threats to organizational assets are distributed between different targets, such as networks, software, data and physical components. Typically, the threats are divided between natural disasters and human acts, where the threats caused by humans can be malicious or non-malicious. Some typical examples of malicious human threats are theft, loss or destruction of an organizational asset, fraud, unauthorized access to the network services, infection with malicious code, disclosure of someone's personal data and identity theft.[1] From most reports, it is obvious that the number of security and privacy incidents is growing. According to the 2007 CSI Survey, insider abuses of network access, viruses and laptop/mobile device theft are the top three types of security attacks (CSI, 2007).

There are different types of humans doing the malicious acts. They can be categorized as for objectives, access,

[1] An identity theft is the illegal use of an individual's personal identifying information (such as name, address, date of birth, credit card number, etc.) to impersonate that person and commit financial fraud.

Download English Version:

https://daneshyari.com/en/article/1026252

Download Persian Version:

https://daneshyari.com/article/1026252

Daneshyari.com