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.

resources, expertise and risk (Schneier, 2004). Each type attempts to compromise the security for a variety of reasons, such as renowned, publicity, gaining competition advances, personal satisfaction, financial gain, revenge, espionage and terrorism. The most known types are hackers, lone criminals, malicious insiders, industrial espionage, organized crime and terrorists.

The economic consequences of security breaches are considerable.[2] Currently, most financial losses are caused by financial fraud, virus (also worms and spyware) and system penetration by an outsider (CSI, 2007). The impact of information security breach is counted as immediate losses and indirect losses. Some typical immediate losses are loss of revenue, loss of productivity and increased costs (overtime costs, insurance premium, etc.). In many situations, actual immediate loss remains a small part of the overall loss of security incidents. Usually, the indirect losses appear to be more serious as they have much longer negative impact on the customer base, supplier partners, financial market, banks and business alliance relationships and those costs are almost as high, and sometimes even higher, than the immediate costs caused by the security breach (Camp & Wolfram, 2004; Dynes, Andrijcic, & Johnson, 2006; Rowe & Gallaher, 2006). Indirect losses present damage to the reputation of the organization, interruption of business processes, legal liabilities, loss of intellectual property and damage to customer confidence.

The loss due to a security breach is typically related to the confidentiality, integrity of the data or availability of information assets. Among them, the impact of confidentiality-related security breaches is associated with most significant losses in the organization assets value (Campbell, 2003; Hovava & D'Arcy, 2003).

However, the data about the true cost of a security incident are very difficult to find. One of the reasons is that most of the organizations do not systematically track and document security incidents. The other reason is that the enterprises deal with the problems internally, fearing a disaster in public relations, a devastating loss of consumer confidence, or worse, revealing vulnerability to other hackers. Currently, the most up-to-date actual data come from different annual survey reports (CERT, 2007; CSI, 2007; DTI, 2006). These reports are a summary of an inquiry where the businesses are reporting about the cost that occurred after various categories of security incidents over a year.

2.3. Identification of the vulnerabilities

Vulnerability is a weakness in security procedures, technical controls, physical controls or other controls of an asset that a threat may exploit. Most security incidents are caused by vulnerabilities presented by flaws in software. Statistics reveal that the number of vulnerabilities reported has increased dramatically over the years, from only 171 in 1995 and 1090 in 2000 to 8064 in 2006 (CERT, 2007).

Vulnerabilities are typically known as a technical issue; however, there are vulnerabilities caused by human factor. This type of vulnerabilities are caused by users sharing their passwords or using weak passwords, by not understanding or ignoring security policies, opening non-trusted e-mail, visiting web sites, or downloading software that contains malicious code.

Software vulnerability disclosure has become a very critical area of concern and has caused a hot debate between scientists (Anderson & Schneier, 2005; Kannan & Telang, 2004). Those in the open-source communities argue that openness helps to defend the assets better and more (Arora & Telang, 2005), while other researchers and software vendors claim that openness is more valuable to attackers (Rescorla, 2004).

One mechanism for ensuring security is to define vulnerabilities as tradable externalities and the specific good, which are considered the medium of exchange in various vulnerability markets (Camp, 2006). This means a vendor or system owner offers a reward for the first person who illustrates vulnerability and the reward can be increased as time passes and the system owner becomes more certain of security. An alternative mechanism is an auction where a person with knowledge of a vulnerability announces its existence, while others indicate a willingness to pay for it (Ozment, 2004).

Some organizations on a vulnerability market act as infomediaries, which openly buy vulnerabilities (e.g. iDefense and Tipping Point). The infomediary then shares this information with its subscribers. The infomediary may deliver a patch for the vulnerability or provide filters to protect against attacks that exploit the vulnerability. In this way, subscribers can protect themselves against attacks that exploit those specific vulnerabilities. The Computer Emergency Response Team (CERT) in contrast does not pay or charge anything for vulnerability. CERT is acting as an infomediary between friendly identifiers who voluntarily, with no explicit monetary gains, report vulnerability information and the software users. In order to ensure that such public notifications are not exploited by attackers, CERT contacts the vendor for the appropriate patch and waits for the convenient time before publicly disclosing the vulnerability.

The overall question arises, why software vendors do not make their products more secure on the first place. The answer lies in economics. The security of software products is difficult to measure and users hardly differentiate between the more secure and the less secure products (Anderson, 2001). The costs of adding good security to software products are big, while the costs of ignoring security are minor (Schneier, 2004). Because vendors are unable to effectively charge a premium for extra security, users are not willing to pay for it and vendors have a little incentive to increase the security of the products. Software

[2]The average annual loss reported in the year 2007 has been doubled from that of the previous year (CSI, 2007).

market suffers from the information asymmetry and is often described as a market for lemons.[3]

To fix vulnerabilities in software products, vendors release patches. According to the CERT, around 95% of security breaches could be prevented by keeping systems up-to-date with appropriate patches. The time window between identification of vulnerabilities and creation of exploits has shrunk dramatically over the years. Therefore, organizations must act fast and apply patches to the system as soon as they are released by the vendor in order to avoid damages due to malicious acts (August & Tunca, 2005; Cavusoglu & Zhamg, 2006). However, it is known that, many systems are still left unpatched for months, even years, and the consequences of not updating systems promptly with necessary patches can cause severe damage (Shostack, 2003). An example is the Nimbda worm, which infected 2.2 million computers in the first 24 h after its appearance, but the patch fixing this vulnerability was released nearly 1 year before the incident (Dacey, 2003). Some other examples where patch fixing the vulnerability was available a long before the incident are SQL Slammer worm, Code Red worm and Blaster worm.

3. Approaches for security risk assessment

Once security risks have been identified, they must be assessed as to their potential loss and to the probability of occurrence. Risk assessment is the determination of the potential impact of an individual risk by assessing the likelihood that it will occur and the impact if it should occur. It helps organizations taking decision regarding the necessary investment in security controls and systems in areas that maximizes the business benefit.

There are many different methodologies for assessing risks. Quantitative risk analysis attempts to assign numeric values to the likelihood and impact of the risk and to the costs and benefits related to the introduction of security controls and systems. The purpose of security control is to mitigate the risk up to a point where the marginal cost of implementing controls is equal to the value of additional savings from security incidents. In contrast to the quantitative approach, the qualitative risk analysis attempts to calculate relative values, instead of assigning exact financial values to assets, expected losses, and cost of controls and systems. Qualitative risk analysis is usually conducted through a combination of questionnaires and collaborative workshops.

Both qualitative and quantitative approaches have their advantages and drawbacks. The problem with the quantitative risk analysis is in non-existence of a standard method that will effectively calculate the values of the assets and the cost of the controls and systems required to be applied. The advantage of a qualitative approach is in that the process itself demands less staff and the accurate calculation of the asset value (AV) and the cost of control is not required. The drawback of the qualitative approach is in the resulting figures that are usually vague as they are derived as relative values of the assets. Typically, small-size organizations with limited resources usually will find the qualitative approach more convenient.

There are many different security risk assessment methods and techniques. CERT proposed a risk assessment mechanism named OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), which enables the risk evaluations to be carried out in line with the organization size and in line with the available expertise in the organization. Some other popular security risk assessment methods are FAA (Federal Aviation Administration) Security Risk Management, Facilitated Risk Assessment Process (FRAP) developed by Tom Peltier (Peltier, 2005), CCTA Risk Analysis and Management Method (CRAMM) developed by the UK Government's Central Computer and Telecommunications Agency (CCTA) and National Security Agency's (NSAs), INFOSEC Assessment Methodology (IAM) (Douglas, 2006).

3.1. Quantitative risk metrics

The exposure to a risk could be measured with different quantitative metrics. A simple analytical method for risk exposure proposes calculation of annual loss expectancy (ALE). The first thing in ALE calculation is determination of the monetary loss associated with an impact, or the *single loss exposure* (SLE). The SLE is the total amount of revenue that is lost from a single occurrence of the risk. It is a monetary amount that is assigned to a single event that represents the organization's potential loss amount if a specific threat exploits the vulnerability. Unfortunately, determining the impact can be quite difficult for immaterial assets.

The SLE is calculated by multiplying the AV with the *exposure factor* (EF).

$$\mathrm{SLE} = \mathrm{AV} \times \mathrm{EF} \tag{1}$$

The EF represents the percentage of loss that a realized threat could have on a certain asset. AV is the monetary value of the asset. An oversimplified example that explains the approach is in a case when the e-commerce web server has an AV of €50,000, and a virus infection that has affected the server results in estimated loss of 35% of the value, then the SLE in this case is calculated and as a value of €17,500.

Once the SLE has been calculated for a risk, determining the likelihood of a risk occurring is proceeding. The *Annual Rate of Occurrence (ARO)* is the number of times that an organization reasonably expects particular risk to occur during 1 year.

Security risk exposure is calculated by multiplying the ARO and SLE. The product is called the ALE, which represents the total amount of money the organization

[3] A Nobel prize-winning economist George Akerlof employed the used car market as a metaphor for a market with asymmetric information and called it the market for lemons (Akerlof, 1970).

could one lose in 1 year if nothing is done to mitigate the risk:

$$ALE = SLE \times ARO \quad (2)$$

Calculating estimations for SLE or ARO is very difficult. In the area there are very little actuarial data available, as only few companies successfully track the security incidents and report on them. The most accurate information published so far appears to be the information in the tables created from insurance claim data, academic research, or independent surveys (CERT, 2007; CSI, 2007; DTI, 2006).

For example, if a virus infection at the e-commerce web server results in €17,500 in damages, and the probability of a virus infection has an ARO value of 0.5 (indicating once in 2 years), then the ALE value for the owner of this e-commerce server would be €17,500 × 0.5 = €8750).

4. Risk minimization strategies

Once risks have been identified and assessed, the organization must choose the right strategy to minimize the risk (NIST, 2002). The strategies include the following:

- *Avoiding the threats and the attacks* by eliminating the source of risk or the asset's exposure to the risk. This is usually applied in cases when the severity of the impact of the risk outweighs the benefit that is gained from having or using particular asset; e.g. full open connectivity to Internet.
- *Reducing* the asset's exposure to the risk by implementing appropriate technologies and tools (such as firewall, antivirus systems, etc.) or adopting appropriate security policies (like passwords, access control, port blocking, etc.). Mitigation is the primary risk management strategy.
- *Transferring* the risk responsibility by partially shifting the risk to either outsourcing security service provision bodies or buying insurance (Böhme & Kataria, 2006). This way of transferring the risk is becoming, in the last period, an increasingly important strategy for applying security measures within the organization.
- *Accepting* the security measures as a cost of doing business. Risk retention is a reasonable strategy for risks where the cost of investment or insuring against the risk would be greater over time than the total losses sustained.

Ideal use of these strategies may not be always possible and sometimes may involve trade-offs or using a combination of two strategies (Bosworth & Kabay, 2002). The strategies are presented in Fig. 1. Security risk assessment can be divided into four regions, which are defined by three boundaries. The first boundary defines the minimum ARO value, under which the risk of threat can be accepted. For example, one could ignore risks with occurrence value less than once in 1000 years. The second boundary is the maximum SLE, above which the impact may have a catastrophic consequences. For this type of threat, one possible solution is transferring the risk to insurance company or reducing the occurrence value under the boundary limit. The third boundary is the maximum ALE value, which defines threat avoidance. The remaining risks can be mitigating by security investments. Fig. 2 illustrates the procedure and the steps in minimization security risks.

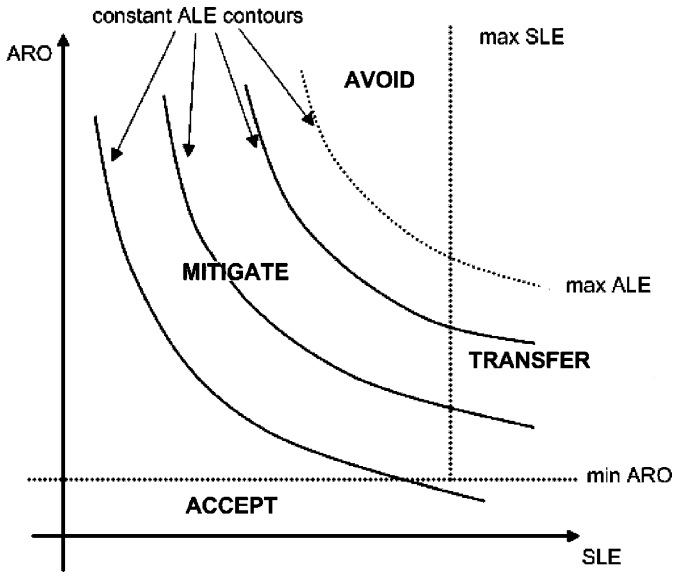


Fig. 1. Risk minimization strategies.

4.1. Information security investment

Reducing risks through investment in security technologies is primary risk management strategy. The purpose of the investment is to lower the probability and consequences of security breaches. However, the investments are not very high. According to the CSI (2007) survey, the average indicated is around 3–5% of the organization's IT budgets that is being spent on security and less than 1% of IT security budget is spent on awareness training (CSI, 2007).

One of the reasons may be the lack of general and reliable models that organizations could use in making decisions about how much is the optimal and most appropriate investment in security controls and systems. The second reason is that most organizations still treat the spending on information security as a pure spending rather as an investment.

The optimal level of information security investment depends on the cost–benefit analysis.[4] In many different models, the costs of information security investment are compared to the expected benefits (Gordon & Loeb, 2002; Schechter, 2002). As long as the benefits exceed its costs,

[4]Some researchers are suggesting a cost-effective analysis, rather than a cost–benefit analysis, as the costs and benefits are not commensurate (Geer, 2002).

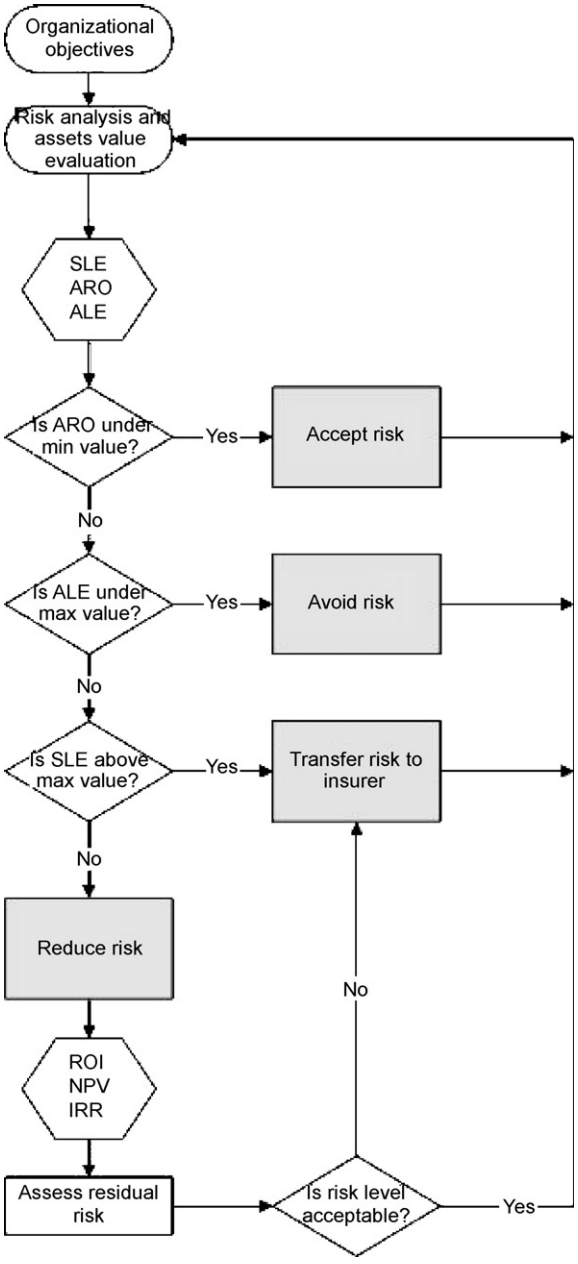


Fig. 2. The procedure for choosing the right strategy to minimize the risk.

the investment in security solution is reasonable. On the other hand, it makes no sense to spend more on security solution than the original cost of the problem. An alternative method that tries to analyze the optimal information security investment is based on the so-called game theory. This theory uses the interaction between a potential hacker and the organization and tries to explain situations of intrusions where the hacker has a motive to attack and cause damage to particular organization (Cavusoglu, Mishra, & Raghunathan, 2004).

Most of the currently used metrics for quantifying the costs and benefits of computer security investments are based on the calculated indicators such as return on investment (ROI), net present value (NPV), internal rate of return (IRR) or combinations of all of them.

4.1.1. Return on investment (ROI)

ROI is a popular accounting metric for comparison of business investments. ROI simply defines how much an organization gets from the spent amount of money. Therefore, ROI can help an organization to decide which of the possible options gives the most value for money invested. For example, a company might use ROI when deciding whether to invest in internal development of a new technology/solution or to purchase a commercial product/solution. The indicator is expressed as a percentage of the returned investment over a specific amount of time. ROI equals the present value of accumulated net benefits over a certain time period, divided by the initial costs of investment:

$$\mathrm{ROI} = \frac{\mathrm{Benefits} - \mathrm{Cost\ of\ investment}}{\mathrm{Cost\ of\ investment}} \tag{3}$$

A simple example: if a new e-commerce web server costs €10,000 and is expected to bring in €50,000 income over the course of 4 years, the ROI for the 4-year period is 400%.

The cost of information security investments should be considered as a compound of the system configuration specific costs and the operating costs. System configuration specific costs are typically one-time spend costs for purchase (or development), testing and implementation of defense solution that protects information assets from possible threats. Operating costs are represented by annual maintenance (upgrades and patching of the defence solution), training users and network administrators, monitoring the solution (Mizzi, 2005). The valid number for cost of security investment can be generated quite easily.

On the other hand, it is very difficult to define, assess or measure the benefits. Firewalls, IDS, antivirus software and other security solutions simply do not generate revenue that can be measured. Therefore, the benefits resulting from information security investment are measured as cost savings that result from preventing information security breaches (Gordon & Loeb, 2006). Benefits can be therefore represented as a difference between ALE without security investment and ALE with security investment:

$$\mathrm{Benefit} = \mathrm{ALE}_{\mathrm{without\ investment}} - \mathrm{ALE}_{\mathrm{with\ investment}} \tag{4}$$

Typically, the initial benefits will rapidly increase with investments and later the benefit growth is stabilized due to the reduction of the probability of security breaches. On the other hand, the cost of security investment could be initially low, but later it can increase due to the needs for higher levels of security infrastructure in the organization. The organizations should invest in security solutions up to the point where the net benefits (i.e., benefits minus costs) are at maximum. In the Gordon–Loeb model the optimal investments in information security are ranging from 0% to 36.8% of the potential loss due to a security breach (Gordon & Loeb, 2002). Later it was also found that in some special scenarios investments up to 50% (or even up to 100%) of the AV are allowed (Willemson, 2006).

This model had also been successfully used in some empirical analysis (Tanaka, Liu, & Matsuura, 2006; Tanaka, Liu, Matsuura, & Sudoh, 2005).

A simple equation for calculating the return on security investment (ROSI) is as follows:

$$\text{ROSI} = \frac{\text{ALE}_{\text{without investment}} - \text{ALE}_{\text{with investment}} - \text{Cost of investment}}{\text{Cost of investment}} \tag{5}$$

The calculation of an example is illustrates as follows: the ALE of the threat of virus infection on a web server is €8750, and after the purchase and implementation of a €1600 worth antivirus safeguard the ALE is valued at €3400. The annual cost of maintenance and operation of the safeguard is €450, so the ROSI in the first year is

$$\frac{(€8750 - €3400 - €1600 - €450)}{(€1600 + €450)} = 160\%$$

While ROI tells what percentage of return will be provided with the investment over a specified period of time, it does not tell anything about the magnitude of the project. So while a 124% return may seem attractive initially, would you rather have a 124% return on a €10,000 project or a 60% return on a €300,000 investment?

4.1.2. Net present value (NPV)

In the case of long-term investments, the time attribute presents a problem in calculating the ROI and managers are mainly using the index known as NVP along with ROI to justify expenditures. The NPV is a financial metric for comparing benefits and costs over different time periods. The methodology behind NPV is in discounting all anticipated benefits and costs to today's value, where all benefits and costs are expressed in a monetary unit (e.g., Euros) (Gordon & Loeb, 2006).

The essence of the NPV is to compare the discounted cash flows associated with the future benefits and costs to the initial cost of an investment. The NVP gives the value of the cash return that is expected and is calculated by summation of the present net value of the benefits for each year over expected n lifetime periods and by subtracting the initial costs of the project. Suppose B_t is the present value of the net benefits of period t, C_t all costs and i the internal rate of discount. The NPV of the investment is calculated as follows:

$$\text{NPV} = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} \tag{6}$$

A positive NPV means that the project generates a profit, while a negative NPV means that the project generates a loss. Therefore, a project is profitable, if the NPV is greater than zero. The NPV is useful in cases when alternatives are being evaluated. For example, an organization chooses between two security solutions where one costs €15,000 in advance and the other costs yearly €5000 for 3 years. Both solutions cost €15,000, but the second solution is better because organization can invest the remaining money in other places for a defined time. Therefore, the real cost of the second solution is less than €15,000.

An important characteristic of NPV is that it provides with information about the cash value of the expected return and therefore indicates the magnitude of the project; the drawback is in the lack of information about the time the expected return occurs.

4.1.3. Internal rate of return (IRR)

Like the NPV, the IRR is often used to analyze long - term investments. The IRR equals the percentage discount rate that makes the NPV of the investment equal to zero:

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+\text{IRR})^t} = 0 \tag{7}$$

IRR is particularly useful when a multi-year investment is made with costs that change radically from 1 year to the next. But like ROI, IRR does not give any indication of the magnitude of the project involved.

Each of these financial measures has its own strengths and weaknesses. The ROI is intended to be used for evaluating past investments, in contrast to the NPV and IRR, which are typically used to make decisions about potential new investments (Gordon & Loeb, 2006). ROI has the difficulty in defining what the magnitude of the investment is and, unlike the NPV or IRR, the ROI does not consider the time value of money. However, calculating ALE is more difficult for the NPV and IRR. In most cases, the NPV and IRR are better indicators than a simple ROI calculation (Gordon & Richardson, 2004). To get a clear and complete picture of a prospective investment, the standard approach should be based on all of these measures.

Although ROI has a number of limitations, when compared with NPV and IRR, ROI is still by far the most popular metric used. According to the 2007 CSI Survey, 39% of organizations use ROI as metric, 21% of them use NPV and 17% use the IRR (CSI, 2007).

4.1.4. A practical illustration

The illustration of the process of comparison between alternatives using cost–benefit analysis is provided in the next example. An organization with 500 computers is decided to reduce the security risk. It is estimated that the potential annual loss from security breach would cost the organization €1,000,000. The current implemented information security controls reduces the security risk by 80%, but this is not good enough. The organization's security goal is to reduce the probability of security breach to max 10%. The investment is intended for 4 years; after that period, the state of security in the organization will be evaluated again.

The organization wants to choose between three alternatives. The first alternative is a low-cost security solution (LC), which reduces the probability of a security breach to 10%, which is just within the limits of security objectives. The purchase price of this solution is €60,000 and organization

estimate €20,000 for yearly maintenance costs for in-house technical staff (updates, monitoring and upgrades).

The second alternative is professional solution (PRO), which reduces the probability of a security breach to just 1%. Its purchase price is €100,000, while the annual renewal price is €30,000. Because this is a more professional solution, the technical staff needs training, which costs €30,000, but further yearly maintenance costs will be smaller, just €5000.

The third alternative is outsourcing the additional security (OUT). The company providing outsourcing service assures that a probability of security breach is no more than 7%. The company charges €150,000 for implementing security solution and €25,000 for annual maintenance and support. There is no need for extra in-house technical support.

Benefits for each alternative can be simply calculated by using the ALE and the promised reduction in probability of security breach:

$$\text{Benefits}_{(LC)} = €1{,}000{,}000 \times (90\% - 80\%) = €100{,}000$$
$$\text{Benefits}_{(PRO)} = €1{,}000{,}000 \times (99\% - 80\%) = €190{,}000$$
$$\text{Benefits}_{(OUT)} = €1{,}000{,}000 \times (93\% - 80\%) = €130{,}000$$

In Table 1 the benefits are represented together with the costs for all alternatives.

The first comparison is calculating the ROI. From Eq. (3) we get the results:

$$\text{ROI}_{(LC)} = 186\%$$
$$\text{ROI}_{(PRO)} = 176\%$$
$$\text{ROI}_{(OUT)} = 108\%$$

So far it looks like LC solution is the favorite, but, as was shown above, the ROI provides information on the percentage of the value of return only and not on the actual magnitude. Furthermore, ROI does not consider the time value of money. In this case, Eq. (6) is used for calculating the NPV, and the NPV calculation gives a solution different from that provided with the ROI calculation:

$$\text{NPV}_{(LC)} = €223{,}676$$
$$\text{NPV}_{(PRO)} = €416{,}289$$
$$\text{NPV}_{(OUT)} = €222{,}325$$

The final comparison is done with a calculation of the IRR from Eq. (7). The IRR confirms the NPV results, and is in favor of PRO solution:

$$\text{IRR}_{(LC)} = 128\%$$
$$\text{IRR}_{(PRO)} = 130\%$$
$$\text{IRR}_{(OUT)} = 59\%$$

The presented example has some limitation, but it can provide an approximate qualitative estimation. The PRO alternative is most expensive, but it also seems the most appropriate choice because NPV and IRR rank it first. The LC alternative has the highest ROI, but this is mainly due to ROI limitations. The results are presented in Table 2.

4.2. Information insurance

One of the strategies by which the organizations may respond to the security risks is by transferring the risk to insurers. Purchasing information insurance allows organizations to reduce risks that remain, even when these organizations are also using technical security solutions. Insurance usually requires minimal investment and provides an environment where every party's risk is a function of the lowest investment. There is a clear economic argument that insurance is an appropriate measure for security mechanisms protection, when the reliability and robustness of those mechanisms depend upon the weakest link (Paxson, 1998). The positive side of using insurance is also that insurance turns variable cost risks into fixed-cost expenses, and organizations like fixed-cost expenses because they can be budgeted (Schneier, 2004).

Information insurance deals with risks of substantial financial losses remaining after technical security measures

Table 2
The comparison between ROI, NPV and IRR calculation

Alternative	ROI (%)	NPV	IRR (%)
LC	186	€223,676	128
PRO	176	€416,289	130
OUT	108	€222,325	59

Table 1
Calculated benefits and costs for all alternatives

Year	Rate	Alternative LC			Alternative PRO			Alternative OUT		
		Benefits (€)	Purchase and upgrade costs (€)	Maintenance costs (€)	Benefits (€)	Purchase and upgrade costs (€)	Maintenance costs (€)	Benefits (€)	Purchase and upgrade costs (€)	Maintenance costs (€)
0			60,000			100,000			150,000	
1	0.05	100,000		20,000	190,000	30,000	40,000	130,000	25,000	
2	0.05	100,000		20,000	190,000	30,000	5000	130,000	25,000	
3	0.05	100,000		20,000	190,000	30,000	5000	130,000	25,000	
4	0.05	100,000		20,000	190,000	30,000	5000	130,000	25,000	

have been instituted. Information insurance coverage against losses from two classes of risk (Gordon, Loeb, & Sohail, 2003).

- First party risks cover losses occurring directly to the insurance holder. They include, for example, loss of profits due to theft of trade secrets, destruction of property (software, hardware and data), business interruption due to hacker or virus attacks and software failures, etc.
- Third party risks cover financial compensation for losses of third parties that occur due to shortcomings in the insurance holder's field of responsibility. For example: damage caused by inadvertently forwarded computer viruses, contractual penalties due to IT failures (because a hacker or virus stopped insecure system), contents placed on the company's web site (infringement of copyrights), theft of information held about a third party such as credit card records.

The leading providers of information insurance in the market today are AIG and Lloyd's of London, which had offered the first specific information security policy in 2003. Before pricing their policies, the insurers need to know what the risks are. Counterpane Internet Security, partner of Lloyd's of London, evaluates an organization to provide metrics to determine if the organization is risk-seeking or has invested rationally in security (Counterpane, 2000).

According to the CSI (2007) survey, only 29% of organizations are using information insurance. This is mainly because insurers have no good actuarial data available on which they base insurance rates. Therefore, they have the incentive to add additional risk premiums and charge more for these policies. Some researchers confirm this and have also ascertained that current available information insurance policies offered by insurance companies are nearly useless (Majuca, Yurcik, & Kesan, 2006).

The main problem still remains that security risks are very hard to quantify. When insurance companies gain experience and good actuarial data, the additional risk premiums would shrink and prices for such policies would become more attractive.

5. Conclusions

Information security risk management is a fundamental concern to all organizations. This paper presents the analysis of the problem associated with determining investment in information security. The outcome of the analysis resulted in a recommendation that could evolve in a standardized approach. The approach starts with the methodical system used in the risk management process, which enables identification of the assets. This provides good understanding of why and what should be protected in a particular organization. The threat analysis provides information about the threats and with what an organization is to confront in the global business processes. The combination of these approaches enables good understanding of the security information protection that may have an impact on the on-going business. In addition to that, the vulnerability analysis shows where and how the threat could occur. By the combination of the identified vulnerabilities and the respective controls that mitigate the risk, the probability of occurrence of the threat can be estimated. After the risk is defined, the financial metrics to evaluate the security investments to mitigate risk can be applied. So far, no standard model for determining the financial risk associated with security incidents exists and the recommendation is for the use of several indexes, combined or modified, due to the circumstances of particular cases as the methods for figuring out the cost of solutions can vary greatly. Some include hardware, software and service costs, while others factor in internal costs, including indirect overhead, and long-term impacts on the productivity. Each of the indexes presented in this paper (ROI, NPV and IRR) have their benefits, but each of them used individually does not present an appropriate solution. Therefore, the best way to assess the required investment is the use of a combination of these methods.

References

Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, *84*, 488.

Anderson, R. (2001). Why information security is hard: An economic perspective. In *ACSAC '01: Proceedings of the seventeenth annual computer security applications conference* (Vol. 358). Los Alamitos, CA: IEEE Computer Society, 2001.

Anderson, R., & Schneier, B. (2005). Economics of information security. *IEEE Security and Privacy*, 12–13.

Arora, A., & Telang, R. (2005). Economics of software vulnerability disclosure. *IEEE Security and Privacy*, 20–25.

August, T., & Tunca, T. (2005). *Network software security and user incentives*. Graduate School of Business, Stanford University August 2005.

Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In *The fifth workshop on the economics of information security (WEIS 2006)*.

Bosworth, S., & Kabay, M. E. (2002). *Computer Security Handbook* (4th ed.). Wiley.

Camp, L. J. (2006). The state of economics of information security. *A Journal of Law and Policy for the Information Society*, *2*(2).

Camp, L. J., & Wolfram, C. (2004). Pricing security. In J. Camp, & R. Lewis (Eds.), *Economics of Information Security* (pp. 17–34). Kluwer.

Campbell, K. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Cavusoglu, H., Cavusoglu H., & Zhamg, J. (2006). Economics of security patch management. In *The fifth workshop on the economics of information security (WEIS 2006)*.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87–92.

CERT (2007). Computer Emergency Response Team Coordination Center (CERT/CC) vulnerability remediation statistics. Retrieved October 20, 2007, from 〈http://www.cert.org/stats/fullstats.html〉.

Counterpane (2000). Counterpane Internet Security, Lloyd's of London: Counterpane Internet Security announces industry's first broad insurance coverage backed by Lloyd's of Londonfor e-commerce and Internet security. Retrieved February 7, 2007, from 〈http://www.counterpane.com/pr-lloyds.html〉.

CSI (2007). CSI Survey 2007. The twelfth annual computer crime and security survey. Retrieved October 10, 2007, from 〈http://www.gocsi.com/forms/csi_survey.jhtml〉.

Dacey, F. R. (2003). Effective patch management is critical to mitigating software vulnerabilities. GAO-03-1138T.

Douglas, J. L. (2006). *The security risk assessment handbook. A complete guide for performing security risk assessments*. Auerbach Publications.

DTI (2006). Information security breaches survey 2006. Retrieved March 18, 2007, from 〈http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf〉.

Dynes, S., Andrijcic, E., & Johnson, M. E. (2006). Costs to the U.S. economy of information infrastructure failures: Estimates from field studies and economic data. In *The fifth workshop on the economics of information security (WEIS06)*.

FIPS (2004). *Federal Information Processing Standards (FIPS) publication 199*. Security Categorization of Federal Information and Information Systems.

Geer, D. (2002). Making choices to show ROI. *Secure Business Quarterly*, *1*(2), 1–5.

Gordon, A. L., & Loeb, P. M. (2002). The economics of information security investment. *ACM*, *5*(4), 438–457.

Gordon, A. L., & Loeb, P. M. (2006). *Managing cybersecurity resources: A cost–benefit analysis*. McGraw Hill.

Gordon, A. L., & Richardson, R. (2004). The new economics of information security. *Information Week*, 53–56. April 13, 2004. Retrieved February 11, 2007, from 〈http://www.banktech.com/aml/showArticle.jhtml?articleID=18901266〉.

Gordon, A. L., Loeb, P. M., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *ACM*, *46*(3), 81–85.

Hoo, S. (2000). *How much is enough? A risk-management approach to computer security*. CA: Stanford University.

Hovava, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements of the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

ISO (2005). Information technology—Security techniques—Information security management systems—Requirements, ISO/IEC 27001:2005.

Kannan, K., & Telang, R. (2004). An economic analysis of market for software vulnerabilities. In *The third workshop on the economics of information security (WEIS04)*.

Majuca, R., Yurcik, W., & Kesan J. P. (2006). The evolution of cyber insurance. In *ACM Computing Research Repository (CoRR)*. Technical report cs.CR/0601020.

Microsoft (2004). Microsoft security Risk Management Guide. Retrieved March 14, 2007, from 〈http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx〉.

Mizzi, A. (2005). Return on information security investment. Are you spending enough? Are you spending too much? InfosecWriters.

NIST (2002). *Risk management guide for information technology systems*. National Institute of Standards and Technology (NIST) Special Publication 800-30.

NIST (2004). *MAPPING types of information and information systems to security categories*. National Institute of Standards and Technology (NIST) Special Publication 800-60.

NIST (2008). *NIST Special Publications (800 Series)*. Retrieved February 11, 2008, from 〈http://csrc.nist.gov/publications/PubsSPs.html〉.

Ozment, A. (2004). Bug auctions: Vulnerability markets reconsidered. In *The third workshop on the economics of information security (WEIS04)*.

Paxson, V. (1998). Bro: A system for detecting network intruders in real-time. In *Proceedings of the 7th Usenix security symposium*, January 1998.

Peltier, T. (2005). *Information security risk analysis* (2nd ed.). Boca Raton, FL: Auerbach Publications.

Rescorla, E. (2004). Is finding security holes a good idea? In *The third workshop on the economics of information security (WEIS04)*.

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.

Schechter, S. E. (2002). Quantitatively differentiating system security. In *The first workshop on economics and information security (WEIS)*.

Schneier, B. (2004). *Secrets & lies, digital security in a networked world*. Wiley Publishing.

Shostack, A. (2003). Quantifying patch management. *Secure Business Quarterly*, *3*(2), 1–4.

Tanaka, H., Liu, W., & Matsuura, K. (2006). An empirical analysis of security investment in countermeasures based on an enterprise survey in Japan. In *The fifth workshop on the economics of information security (WEIS06)*.

Tanaka, H., Liu, W., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, *24*, 37–59.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91–95.

Willemson, J. (2006). On the Gordon & Loeb model for information security investment. In *The fifth workshop on the economics of information security (WEIS06)*.



Rok Bojanc is currently CIO of ZZI, a software solution firm active in e-business exchange area. He has been involved with IT and information security for over 10 years. Prior to ZZI, Mr. Bojanc spent over 9 years as instructor; he has written several training courses for subjects including IT, networks, security, and Microsoft server systems. He is a frequent lecturer and speaks about IT and security on many seminars and conferences. As both a technical lead and project manager, he has worked in designing, developing, implementing and managing information systems/networks for more than 7 years. He has written many handbooks and technical articles related to IT. In addition, he teaches undergraduate courses in the areas of information science. He holds a Master's degree in Physics from University of Ljubljana and is pursuing his Ph.D. on Information Management. He is a Microsoft Certified System Engineer (MCSE).



Borka Jerman-Blažič holds an MS in Electrical Engineering from the University of Ljubljana and a Ph.D. in natural and computing sciences from the University of Zagreb.

Prof. Dr. Borka Jerman-Blažič is a full professor at the University of Ljubljana, Department of Economics and is heading the Laboratory for Open Systems and Networks at Jožef Stefan Institute.

She is teaching undergraduate courses in electronic communications and information security and postgraduate courses in Telecommunication Services and Technologies, Legal aspects and standards in ICT and E-commerce. Prof. Dr. Borka Jerman-Blažič is a member of the IEEE Computer Society, a member of the ACM, member of the New York Academy of Science since 1991, member of IFIP. She is appointed member to UNECE/CEFAT UN (Economic Commission for Europe) group for Internet enterprise development, appointed member of eTEN management committee of EU and a member of EU FP7 Programming Committee on Security, Chair (2004–2007) of the Internet Society of Europe (www.isoc-ecc.org), Distinguished Member of Slovene Society for Informatics, member of the editorial board of the international journal of Technology Enhanced e-Learning. She is holding Plaque of appreciation of the Thai branch of IFIP and ACM for her services in Internet development and awards for best papers (IARIA IEEE conference).

Prof. Dr. Borka Jerman-Blažič has been involved in more than 150 international conferences and workshops as a speaker, invited speaker and chair or a member of the programming committees. She has published more than 90 papers in refereed scientific journals, 154 communications on scientific meetings, 15 Chapters in scientific books, 6 books and other 142 scientific contributions. She has as well experience in editorship from books published by Kluwer P.C and IOS Press (2001–2004).