A Quantitative Model for Information-Security Risk Management

Rok Bojanc, ZZI
Borka Jerman-Blažič, University of Ljubljana

Abstract: Information-security risk management is becoming an increasingly important process in modern businesses. The proposed model for managing information-security risks is based on a quantitative analysis of the security risks that enable organizations to introduce optimum security solutions. The model is designed as a standard procedure to lead the organization from the initial selection of input data to the final recommendations for the selection of the appropriate solutions, which reduces a certain security risk. In analyzing the security risks, the model quantitatively evaluates the information assets, their vulnerability, and the threats to information assets. The values of the risk parameters are the basis for selecting the appropriate risk treatment and the evaluation of the various security measures that reduce security risks. Economic indicators are determined for each security measure in order to enable a comparison of the various security measures. This includes the possibility of investing in technology-security solutions, the introduction of organizational procedures, and the training and transfer of risk to an outsourcing provider or to an insurance agency. The model was tested using empirical examples with data from a real business environment.

Keywords: Risk Management, Risk Assessment, Information Security, Optimal Investment, Quantitative Evaluation

EMJ Focus Areas: Risk Management, Quantitative Methods and Models, Operations Management

The Internet is a public space in which the availability and security of e-business and e-commerce operations is guaranteed by the infrastructure security for the operators, and the software and data security for the authorized users and owners. As a consequence, individual, corporate, and government assets are taking an increasingly dematerialized form, as the storage of digital data is becoming equivalent to productivity gains in all respects. The volume of data and information doubles each year, while the value of these corporate and government assets is increasingly derived from, or encapsulated in, this digital, cultural, and industrial asset base.

Trends like globalization, higher productivity, and reducing costs make business organizations increasingly dependent on their information systems and Internet services. A potential attack on information systems and an eventual crash may cause heavy losses relating to data, services, and business operations. Security risks are present in an 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 that are designed to protect the confidentiality, integrity, and availability of information assets. Due to an increasing awareness regarding the potential risks of attacks and breaches, the investments in information security are increasing and taking different approaches depending on the area of applications. Although security technologies have made great progress in the past ten years, the security levels of computers and networks have not seen the same levels of improvement.

In the past, information about security-risk management was not given much attention. A threat was countered by seeking a technical solution to prevent this threat; however, about a decade ago, a number of researchers began to realize that information security is not a problem that can be resolved by technology alone. As a result, they tried to include the economic point of view in the equation. This approach enables business managers to develop a better understanding of security investments, because a technical analysis of the implications of security failures was replaced by an analysis of economic losses (Acquisti et al., 2006). This is the reason why security-aware organizations are shifting the focus from what is technically feasible to what is economically optimal in terms of the prevention of potential failures (Schneier, 2004; Anderson, 2001; Anderson and Schneier, 2005).

Knowledge of information-security risk management opens up many questions about which the presented model can provide answers (Gordon and Loeb, 2002): How to provide security for IT-based operations? Which security level is adequate? How much money should be invested in security? Organizations tend to seek answers to these questions in the framework of risk management.

Information-security risk management is the overall process that integrates the identification and analysis of risks to which an organization is exposed, provides an assessment of the potential impact on the business, and enables a decision regarding the action to be taken so as to eliminate or reduce the risk to an acceptable level (NIST, 2004, 2005). It requires a comprehensive identification and evaluation of the organization's digital assets, the consequences of security incidents, and the likelihood of successful attacks on the systems exposed to the digital world, as well as a cost-benefit analysis of the security investments (Soo Hoo, 2000). Standards and guidelines are available for information-security management, such as the ISO 27000 (2009) series and various NIST publications; however, advancements in the field of technology require more sophisticated decision-making approaches when it comes to security-technology investments as well as data- and digital-asset protection (Gordon and Richardson, 2004).

Practicing engineering managers must be able to manage security risks in order to develop products and solutions that meet customers' demands. This article presents a novel model for information-security risk management that is based on a quantification of the enterprises' resources and the measures required to protect these assets using known economic indicators. The quantitative model and the method improve the practice of engineering management and help engineering managers make a decision on the necessary investments in security measures

Refereed Research Manuscript. Accepted by Special Issue Editors Pinto and Bozkurt

that are the most effective for a given situation. The model is designed as a standard procedure that leads engineering managers from the initial selection of the input data to the final recommendations for the selection of an optimum measure that reduces a certain type of security risk. The advantage of using this model is in the completeness of the considered security measures that encompass not only the protection technology but also the organizational approaches, the education of employees, the insurance possibilities, or outsourcing solutions. The model provides good guidelines for practical use. The usability of the model is illustrated with several examples of possible security incidents and the chosen measures.

Related Research

Information security was traditionally considered to be a technical discipline, whose purpose was to provide the maximum level of security (McGraw, 2006). In the past decade, however, a major economic component began to be considered in the related research as the investments in information security rapidly increased (Anderson, 2001). Information-security economics, a relatively new field of study, uses economic theory and models to analyze the incentives between the involved stakeholders. Cavusoglu (2004) argues that information security should be viewed not just as a cost, but as a value creator that supports and enables e-business operations. Cavusoglu (2004) claims that a secure environment for information and transaction flows can create value for companies and their partners. An analysis of investments in information security requires a quantification of the costs and benefits of the investments in a comparable way. The cost of an investment includes the price of the required hardware, software, and labour (among others); however, it is more difficult to quantify the benefits. At the same time, it is important that the investment value is not higher than the value of the protected asset.

An estimation of the total cost of security breaches can be made in several ways. Some approaches try to quantify the short-term and long-term costs, or the tangible and intangible costs, while other methods use the market-efficiency theory and the capital market valuation of companies to quantify the costs (Bojanc and Jerman-Blažič, 2008). The loss in market value in the days surrounding the announcement of an accident is just an approximate value of the true cost of the security breach (Farahmand, 2003).

Farahmand (2003) suggests a simple probability-based model for the valuation of possible attacks. The probability assessment for each incident is subjective, grading the identified threats on a five-step scale—from very low to very high probability—and assigning the probabilities to the various steps on the scale. The approach is semi-quantitative, because it uses a qualitative approach to obtain quantitative probability estimates. Gordon and Loeb (2001, 2002) propose an economic model that determines the optimum amount to invest in information security by calculating the marginal benefits of information-security investments. An organization should only invest up to the point where the marginal benefits of the investment equal the marginal costs. Whenever the marginal benefit is larger than the marginal cost, the investment should be increased. Willemson (2006), however, emphasizes that the suggested upper limit of the model may not be correct when the model is applied to the general case and to all possible vulnerability functions.

Ryan and Ryan (2006) view security as an inversion of the risk and establish a quantitative approach to measure the gains in security through expected-loss risk measurements. The approach of basing an investment decision on the expected loss is suggested by Gordon and Loeb (2002), and the rule of thumb is that a positive expected net benefit is an attractive investment. The approach is based on the ability to obtain probability distributions for information-security failures. It uses survivor and failure functions, but since the available data are censored and therefore biased, the quality of the results is questionable. For this reason, Ryan and Ryan (2006) introduce the Kaplan-Meier and Nelson-Aalen estimators that can be used instead. The basic assumption is that an investment in security reduces the risk of successful attacks. The advantage of an investment is measured as the difference between the expected losses in the investment or no-investment scenarios. Based on these findings, Bojanc, Jerman-Blažič, and Tekavčič (2012) presented a general mathematical model for a quantitative evaluation of the investments in a variety of security measures and the selection of the optimum security solutions.

McGraw's (2006) view on software security is based on, "the idea of engineering software that continues to function correctly under malicious attacks." In order to solve the problem of software security, McGraw (2006) proposes three pillars: (1) applied risk management, (2) software security touch-points (best practices into the software development life-cycle), and (3) knowledge. He also argues that an ICT system is usually built on the assumption that the system would not be intentionally abused, resulting in the cases of use that describe the system's normative behaviour, predicated on the assumption of the correct usage. Past breaches of information security have resulted in both immediate and indirect losses, with indirect losses having often been more serious than the direct ones. The optimum level of information-security investments is treated on the basis of the expected cost/benefit investment trade-offs. Pinto, Arora, Hall, and Schmitz (2006) introduce a calculation of risk-based return on investment (RROI). RROI pertains to the ratio between the net benefit in implementing an IT solution and the cost of this implementation. Unlike the conventional notion where ROI measures how effectively resources are used to generate a profit, an RROI measures how effectively resources are used to reduce risk. Other recent work that looks at risk management and discusses the mitigation benefit versus cost trade-off was published by Bahill and Smith (2008). Their work focuses on a standard graphical technique for risk analysis.

Security-Risk Management

How secure is an information system? How secure should an information system be? These are tw questions that information-security experts frequently ask. The simple answer to the question of what level of security an organization needs is: good enough security (Sandhu, 2003). Unfortunately, it is very difficult to determine a level that is "good enough" (Geer, 2004). The optimum security level can be understood as the level of security that is acceptable to the organization (Schneier, 2003). This level can be determined through risk management.

Risk is generally defined as a combination of the probability of an event and its consequence (ISO Guide 73, 2009). In the field of information security, risks can be more precisely defined as the potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization (ISO 27000, 2009). Risk is a combination of the threats to one or more vulnerabilities, leading to a negative impact that is detrimental to one or more of the assets. For example, a hacker using social engineering to the employee (i.e., threat), which due

to the poor awareness of the employee (i.e., vulnerability), leads to unauthorized access to computers and a loss of confidentiality and integrity with respect to sensitive information (i.e., impact).

Enterprise risk management is a process of managing exposure uncertainties with a special emphasis on identifying, controlling, and eliminating or minimizing uncertain events that could potentially prevent business goals from being achieved. The process requires the identification and evaluation of information assets, an assessment of the effects of security incidents, an assessment of the likelihood of successful attacks on information systems, and a business assessment of the costs and benefits of an investment in security solutions. Risk management establishes the basic security elements: assets, owner of the assets, threats, vulnerabilities, risks, and measures. Safeguarding assets is the responsibility of owners who place a value on those assets. Threat agents may also place a value on the assets and seek to abuse the assets in a manner contrary to the interests of the owner. The owners of the assets will ayalyze the possible threats in order to determine which ones apply to their environment. The results are known as risks. This analysis can aid in the selection of countermeasures to reduce vulnerabilities, counter the risks and reduce it to an acceptable level (ISO 15408, 2008).

Today, many engineering managers have realized that information security is moving into the management domain from the technical domain (Gordon and Loeb, 2005). Engineering managers already manage different kinds of risk, and the risks associated with information security are just another type of risk. There are many different ways to manage risk. The right one in a given situation depends on the details of each situation.

The process of risk management consists of various stages through which we can identify the vulnerabilities in an enterprise information system, evaluate the potential security protection, decide on the acceptable risk and choose the most appropriate, cost-effective protection. The aim of the process is protection that does not cost more than the expected loss as a result of the attack. The risk-management process usually consists of two main stages: risk assessment and risk treatment.

Overview of the Risk-Assessment Model

To effectively manage information-security risks, we employed a mathematical model that uses a quantitative approach (Bojanc, Jerman-Blažič, and Tekavčič, 2012). Our risk-management model consists of four phases. The first phase is the risk assessment, which identifies and evaluates the vulnerabilities and threats for each information asset and calculates the probability of an incident and the loss due to a security incident. The second phase is the risk treatment, which selects an appropriate treatment for each assessed risk. The third phase is the selection of the security measures and the assessment of the impact that the selected measures have on the risk reduction. The last phase is the comparison of the selected security measures and an economic analysis of the profitability of each measure.

The objective of the risk assessment is to identify and measure the risk in order to obtain the relevant information for the decision-making process. A risk assessment requires good knowledge about the information assets within an organization, the threats to which assets are exposed, and the system vulnerabilities that threats could abuse. To put it simply, the risk-assessment process is a determination of the potential harm to an individual risk and the likelihood that the event might occur.

The model is based on business processes that are supported by information assets. Since there is usually a large number of business processes within an organization, this model focuses only on the core business processes. The risk-assessment procedure identifies and evaluates the vulnerabilities and the threats for every information asset that is part of the business process. The output data of the risk assessment is the risk parameter defined by the probability of the occurrence of a security incident and the consequences of that incident.

A schematic diagram of the parameters for the risk assessment is shown in Exhibit 1. The threat agents contain a set of possible threats (T) that have undesirable effects on the information system. These threats attack the vulnerabilities (v) of the information assets. Successful attacks lead to a security incident (ρ), which represents a financial loss (L).

Identification and Evaluation of the Threats and Vulnerabilities

Information assets are exposed to threats. A threat can be defined as a potential cause of undesired incidents that may cause damage to the system or organization (ISO 27000, 2009). Threats have different impacts on information assets. Basically, the threats focus on:

- The destruction of information assets
- The changing of information assets
- The theft of information assets
- The disclosure of confidential information
- The interruption of service

Threats can exploit vulnerabilities in the software, network configuration, security procedure, etc. The majority of security incidents are caused by vulnerabilities in the software (Arora and Telang, 2005). Although these vulnerabilities are, in most cases, of a technical nature, the reason for the incident is often human in its nature. Examples include the use of weak passwords, the inadequate protection of passwords, the misunderstanding or ignorance of security policies, the uncontrolled opening of attachments in e-mail messages, visits to suspicious websites, or the installation of software that contains malicious code. The standard ISO 27005 (2008) "Information Security Risk Management" classifies threats in the following categories:

- Physical damage: fire, pollution, dust, corrosion, destruction of equipment or media, etc.
- Natural events: seismic phenomenon, volcanic phenomenon, floods, etc.
- Loss of essential services: failure of air-conditioning, failure of water-supply system, loss of power-supply system, failure of telecommunications equipment, etc.
- Disturbance due to radiation: electromagnetic radiation, thermal radiation, etc.
- Compromise of information: eavesdropping, theft of media or documents, disclosure, retrieval of recycled or discarded media, etc.
- Technical failures: equipment failure, saturation of the information system, etc.
- Unauthorized actions: unauthorized use of equipment, fraudulent copying of software, corruption of data, illegal processing of data, etc.
- Compromise of functions: error in use, abuse of rights, denial of actions, etc.

In order to calculate the security risk we need to assess the probability of threats. The *threat probability* T ($0 \leq T \leq 1$) is defined as a probability of an attack on information assets and is equal to the number of attacks per unit of time. The evaluation of

the probability of threats depends on many factors. For example, what the value of the information assets of an organization are for the attacker, which resources are available to the attacker, whether or not the information about the organizational security level is available to the attacker (information about a high level of security may deter the attacker as more resources would be required), and others. The effectiveness of the threat is determined by the vulnerability of the information asset.

Information assets have vulnerabilities that threats could exploit. Vulnerability can be defined as the weakness of an asset or control that can be exploited by a threat (ISO 27000, 2009). Vulnerability can also be seen as increasing the likelihood of a successful attack on the system. For example, leaving a laptop in an unlocked office, instead of in a locked office, significantly increases the vulnerability of the notebook to theft. The probability that the laptop will actually be stolen depends on the presence of threats and vulnerabilities. Vulnerability by itself does not cause loss; vulnerability is just a condition (or set of conditions) that can allow a threat to impact on information assets.

For the purposes of our model we define *vulnerability* v ($0 \le v \le 1$) as the probability of a threat that is successfully implemented in the form of an incident on an information asset. The limit value $v=0$ indicates that the information assets are completely protected and secured, while $v=1$ means the information assets are totally vulnerable.

The connections between threats and vulnerabilities in Exhibit 1 are displayed only linearly to improve the clarity of the diagram. The model also supports multiple vulnerability-threat relation scenarios where one threat is attacking a single vulnerability, one threat is attacking multiple vulnerabilities, and multiple threats are attacking a single vulnerability.

Probability of a Security Incident Occurring.

Some attacks can be successful, resulting in a security incident, while others are not successful. An information security incident is defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (ISO 27000, 2009).

There are different kinds of security incidents. Some incidents result in an abuse of confidentiality, such as the disclosure of personal bank-account details. Incidents can also be related to an abuse of integrity, such as the malicious deletion or modification of business data. Other incidents are related to the abuse of availability, such as Denial-of-Service (DoS) attacks, which prevent authorized users from using business services.

Security incidents are differentiated not only by type, but especially in terms of the impact on the organization. Some incidents only affect part of the business information system, while other incidents have an impact on the entire organization or even several organizations. The incident could cause a chain reaction of incidents or indirect incidents, for example, a loss of confidentiality relating to sensitive information that leads to a loss of customer trust,

The *probability of a security incident occurring* ρ ($0 \le \rho \le 1$) is defined as the product of the threat probability T and the asset vulnerability v.

$$\rho = T \cdot v \tag{1}$$

The function ρ also fulfils two boundary conditions. The incident probability has zero value when there are no attacks (attack probability is zero), and the probability of a security incident is zero when the system is free of vulnerabilities (vulnerability is zero).

Financial Loss Due to a Security Incident

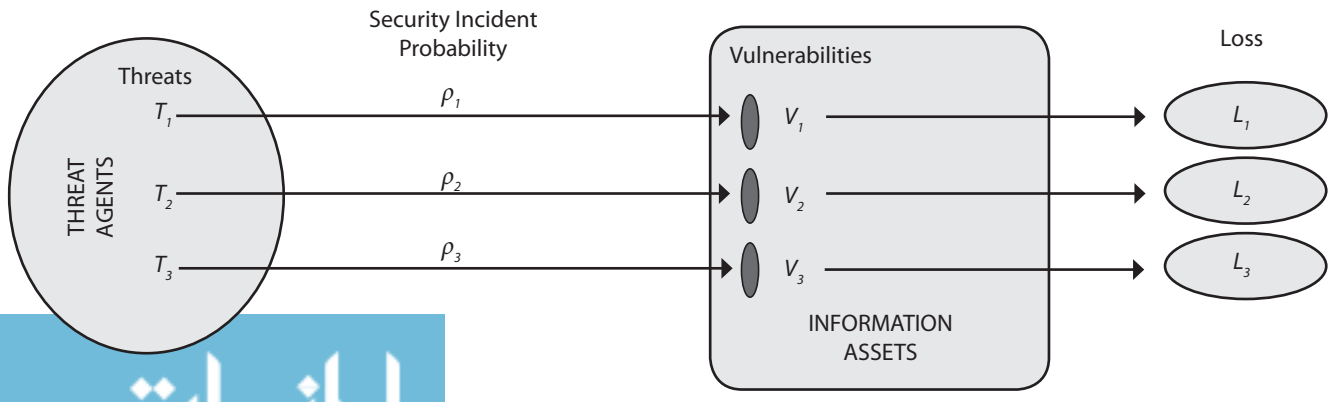
In the case of a security incident, the organization suffers a financial *loss L*. The loss $L>0$ is measured in monetary units (e.g., in euros). The true financial loss of a security incident is difficult to assess; however, it is relatively easy to calculate the immediate direct loss due to an incident. This represents the loss of revenue, loss of productivity, and increased costs. Much more difficult is an assessment of the indirect loss that is sometimes higher than the immediate loss and can also have a much longer negative impact on the customer base, the supplier partners, the financial market, the banks, and business alliance relationships. The quantitative evaluation of loss can be helped by allocating the losses to individual factors and separately calculating the loss of each factor:

$$L = L_s + L_r(t) + L_i(t) + L_p(t) + L_{SLA} + L_{indirect} \tag{2}$$

The *cost of equipment replacement* L_s is the price of new equipment. These types of losses are the easiest to evaluate since the data are usually available or relatively easy to obtain. The cost of repairs in the cases of equipment failure can be significantly reduced by investments in guarantees issued by producers or maintenance-service providers.

The *cost of repairs* $L_r(t)$ is the price of repairs paid to employees or external contractors so as to eliminate the consequences of the security incident and restore the system or the service to normal operation.

Exhibit 1. Risk-Assessment Model



Corporate *income loss* $L_i(t)$ represents a loss suffered on the revenue side due to a system or service failure as a result of the incident.

Organization *productivity loss* $L_p(t)$ is evaluated as reduced business productivity due to system or service failure.

Loss due to non-compliance with statutory provisions or contractual obligations is denoted as $L_{SLA.}$ Its value depends on a contract and/or legislation. For example, the service provider offers its customers a particular service according to a signed SLA contract. In the event that the availability of the offered services is below the limit value specified in the SLA, this represents a cost for the provider, as it must pay back some amount to customers.

Indirect losses $L_{indirect}$ with potential long-term consequences represent damage to the reputation of the organization, the interruption of business processes, legal liabilities, loss of intellectual property, and damage to customer confidence.

A security incident can cause downtime with respect to the information system or services. Downtime consists of the *time to detect* t_d a security incident and the *time to repair* t_r an information system and restore the functionalities of the system. The time t_d is accounted from the moment the incident occurs to the moment that the incident is detected. The factors $L_r(t)$, $L_i(t)$ and $L_p(t)$ in Equation 2 contain a time parameter related to the downtime.

The cost of repairs $L_r(t)$ is evaluated as:

$$L_r(t) = n \cdot p \cdot t_r \tag{3}$$

In Equation 3 n represents the number of employees working to fix the problem and p represents the average wage of an employee working to fix the problem.

The corporate income loss $L_i(t)$ is evaluated as:

$$L_i(t) = EF_i \cdot i \cdot (t_r + t_d) \tag{4}$$

In Equation 4 EF_i represents the reduction in income due to the incident $(0 \leq EF_i \leq 1)$ and i represents the average income per time unit.

The organization's productivity loss $L_p(t)$ I is evaluated as:

$$L_p(t) = m \cdot EF_p \cdot p' \cdot (t_r + t_d) \tag{5}$$

In Equation 5, m represents the number of employees with limited productivity, EF_p represents the reduction in productivity due to the incident $(0 \leq EF_p \leq 1)$, and p' represents the average wage of the employees with limited productivity.

By taking Equations 3, 4, and 5 into account, the factors in Equation 2 can grouped by their time dependency.

$$\begin{aligned} L &= L_s + n \cdot p \cdot t_r + EF_i \cdot i \cdot (t_r + t_d) + m \cdot EF_p \cdot p' \cdot (t_r + t_d) \\ &+ L_{SLA} + L_{indirect} = (n \cdot p + EF_i \cdot i + m \cdot EF_p \cdot p') \cdot t_r + \\ &(EF_i \cdot i + m \cdot EF_p \cdot p') \cdot t_d + L_s + L_{SLA} + L_{indirect} \end{aligned} \tag{6}$$

In order to facilitate the record of further calculations, the factors in Equation 6 can be simplified by grouping the items into three factors.

$$L = L_1 + t_r + L_2 + t_d + L_3 \tag{7}$$

Factor L_3 is expressed in monetary units (e.g., euros), while factors L_1 and L_2 are expressed in monetary units per unit time (e.g., euro/hour).

Calculation of the Security Risk

The risk-assessment procedure identifies and evaluates the vulnerabilities and the threats for each information asset. The risk-assessment output data is the *security risk R,* which represents the expected financial loss caused by the security incident measured in the same monetary unit as L (e.g., euros). The security risk R is defined as the product of the estimated probability of a security incident occurring ρ and the loss due to the security incident L. Taking into account the financial loss in Equation 7 and the likelihood of an incident in Equation 1, the security risk R may be written as:

$$R = \rho \cdot L = T \cdot v \cdot \left[L_1 \cdot t_r + L_2 \cdot t_d + L_3\right] \tag{8}$$

Selecting the Appropriate Risk Treatment

Once the risks have been identified and assessed, the organization must choose the right strategy to minimize the risk. There are multiple options available to deal with each security risk. On the basis of the risk assessment, engineering managers can select one of the possible options:

- *Reduction* of the security risk by implementing appropriate technologies and tools (such as firewalls, antivirus systems, etc.) or adopting appropriate security policies (like passwords, access control, port blocking, etc.). This reduces the probability of a security incident or limits the loss caused by the incident. The reduction is primarily a risk-management strategy.
- *Transfer* of the security risk to either outsourcing security-service provision bodies or an insurance agency. This method of transferring the risk is becoming an increasingly important strategy for applying security measures within an organization.
- *Avoidance* of the security risk by eliminating the source of the 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 a particular asset, e.g., full open connectivity to the Internet. When an engineering manager selects risk avoidance, the organization terminates some activities, but protects them against risk that would have consequences that are considered too serious.
- *Acceptance* of the security risk as a part of business operations. Risk acceptance is a reasonable strategy for risks where the cost of the investment or insuring against the risk would be greater over time than the total losses sustained.

In some cases it is difficult to determine the boundary between each treatment. For example, a firewall can be understood as risk reduction or risk avoidance as well, because the organization renounces the benefits of open networks in order to avoid the risk. Choosing the appropriate treatment of a risk can be quite difficult and often necessitates determining whether or not to employ a compromise and combine the two options. A combination of these measures is also an option. For example, an organization first reduces the risks with an investment, and then either transfers the remaining risk to an insurance agency or assesses the remaining risk to be acceptable, thus introducing no additional measures.

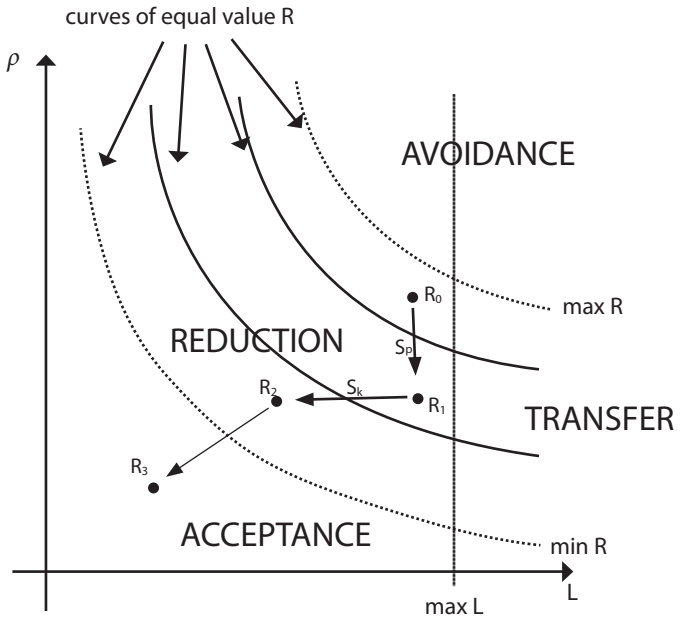
The selection of the appropriate risk treatment can be shown on the diagram $\rho=\rho(L)$ as the probability of the incident and the losses due to the incident, which is shown in Exhibit 2. The curves on this diagram represent the points with the same risk value. The selected risk-treatment option, which reduces the risk R, moves the risk point to a lower risk curve. If the selected risk

treatment reduces the probability of the incident ρ, the risk point is moving vertically downwards from point R_0 to the point R_1 on the diagram; however, if the chosen risk treatment reduces the loss L, the risk point is moving on the diagram horizontally to the left from point R_1 to point R_2.

Each of these risk-treatment options represents a certain area on the graph. It is necessary to define the *risk-parameter limit values* that present the three border lines dividing the area in the graph into four units, where each area corresponds to a specific risk-treatment option. The risk-limit values are specified as follows:

- R_{max} - maximum risk value that is still acceptable for the organization
- L_{max} - maximum one-time loss that is still acceptable for the organization
- R_{min} - minimum risk value that is still meaningful for the organization

Exhibit 2. Risk-Treatment Determination



In a risk-treatment process, the risk-parameter values of R and L are compared to the risk-limit values R_{max}, $L_{max,}$ and R_{min}. The first border line sets the minimum risk value ($R<R_{min}$). Below this value, the risk is negligibly low, so the implementation of a security measure is not financially justified and the risk is accepted. The second border line is the maximum risk value ($R>R_{max}$), above which risk is avoided. The third boundary line is the maximum single loss ($L>L_{max}$) due to the incident. Above this value the impact of the risk can have catastrophic consequences and the recommended risk-treatment option for this area is a transfer of risk. The security risk in the rest of the area ($L<L_{max}$) is treated by reducing risk through an investment in security measures.

Security-Measure Selection and Evaluation

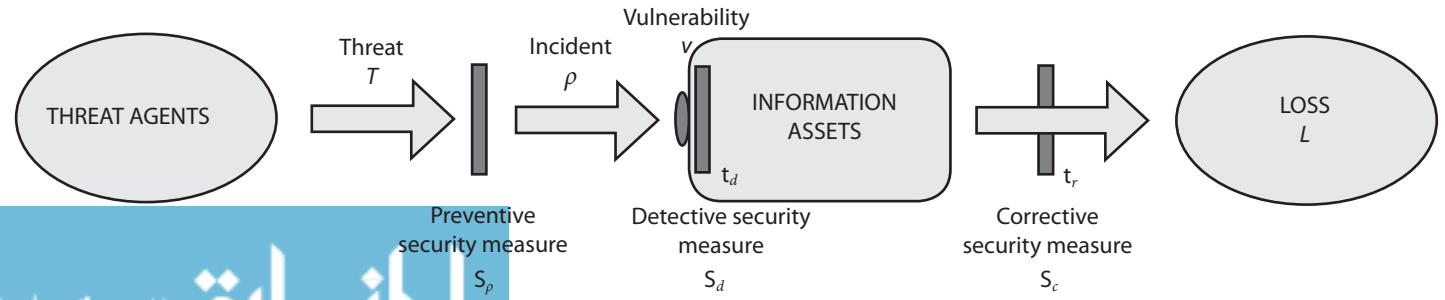
Security measures are activities, procedures or mechanisms to prevent or reduce the damage caused by the realization of one or more threats. These measures may be physical protection, diagnostic sensors, software, algorithms, organization policies or procedures. Many functions can be implemented by security measures, including detection, deterrence, prevention, mitigation, repair, recovery, control, and awareness. The appropriate selection of security measures is essential to ensure effective information security. Exhibit 3 shows how an organization can protect itself against potential security attacks by implementing *security measures* that can be classified into three categories according to their impact on the risk parameters:

- *Preventive security measures* s_p, which reduce the probability ρ of a security incident (e.g., firewall, antivirus protection).
- *Corrective security measures* s_c, which reduce the loss L in the event of an incident (e.g., maintenance contract with subcontractors, plan for continuous operations, back-up data, redundant system, implementation of various standards).
- *Detective security measures* s_d, which reduce the time t_d needed to detect an incident and enable information gathering about the threat (e.g., IDS systems).

The effect of security measures is also shown graphically in Exhibit 3. The introduction of the preventive measure s_p shifts the risk point on the graph vertically downward (from R_0 to R_1) to a lower risk curve, and the introduction of corrective measures s_c and detection measures s_d moves the risk point horizontally on the graph to the left to the lower curve of risk (from R_1 to R_2). Detective security measures enable a detailed analysis of the security events, detect incidents, and warn against them. The use of detective protection enables loss reduction and a more realistic assessment of the attack probability T, and the incident probability ρ. When organizations are not using detective controls, the probability values are merely an estimate and they can differ a great deal from realistic values. Wrong assumptions can also lead to the non-optimal selection of security measures.

Each *security measure* $s(\alpha C)$ is defined by two quantitative parameters: the productivity of measure α and the cost of measure C. *Security measure productivity* $\alpha > 0$ represents the impact of a security measure on the risk reduction. *The cost of measure* C is defined as an investment expressed in some currency (e.g., euros). This takes into account all the expenses related to the

Exhibit 3. Integrating Security Measures into the Model



implementation of the selected security measure, the expenditure in capital investment and the operating costs. An example of capital investment is the purchase of a new system for intrusion detection in a network, which helps to reduce the likelihood of security intrusions in a particular time period. The operating costs are the one-time cost of implementation, the testing and training, the cost of fixes and upgrades, the maintenance costs, and other expenses related to the introduction of a measure.

When introducing security measures, it is always necessary to consider the corporate budget for security investments C_{IT_budget}, which must be above the cost C of an individual measure ($0 \le C \le C_{IT\_budget}$). If the cost of a measure is higher, then the implementation of the measure is not possible. Research by CSI has shown that almost half of organizations spend more than 6% of their overall budget resources on IT security (CSI, 2011).

The introduction of a preventive security measure $s_p(\alpha_p, C_p)$ reduces the security-incident probability ρ. Various incident probability ρ functions for security measures are available (Gordon and Loeb, 2002; Willemson, 2006). In their paper Gordon and Loeb (2002) give examples of incident-probability-function families $\rho(T,v,C)$ that satisfy the boundary conditions: $\rho(0,v,C_p) = 0$, $\rho(T,0,C_p) = 0$, $\rho(T,v,0) = T \cdot v$, $\lim_{C_p \to \infty} \rho(T,v,C_p) = 0$.

Because the preventive security measure s_p reduces the incident probability, it is also the case that $\frac{\partial \rho}{\partial C_p} < 0$ and $\frac{\partial^2 \rho}{\partial C_p^2} > 0$.

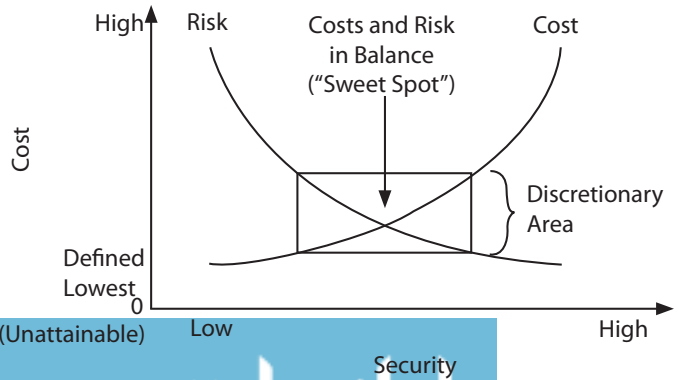
In the presented model we used the Gordon-Loeb second class of security-breach probability functions $\rho(T,v,C)$ that satisfy the above conditions and are quite popular among researchers (Matsuura; 2008, Baryshnikov, 2012):

$$\rho(T,v,C_p) = T \cdot v^{\alpha_p C_p + 1} \tag{9}$$

The loss L resulting from a security incident can be reduced with an investment C_c into a corrective security measure $s_c(\alpha_c, C_c)$, which reduces the repair time t_r and with an investment C_d into a detective security measure $s_d(\alpha_d, C_d)$, which reduces the detection time t_d. Corrective security measures reduce the time to repair, consequently reducing the organization's loss caused by the incident. This is expressed by the following equation:

$$t_r = t_r^{\,0} e^{-\alpha_c C_c} \tag{10}$$

Exhibit 4. Balancing Cost and Security (Source: Kaplan, 2007)



where $t_r^{\,0}$ represents the time needed to repair without the implementation of a security measure. The function t_r is declining and convex: $\frac{\partial t_r}{\partial C_c} < 0$, $\frac{\partial^2 t_r}{\partial C_c^2} > 0$.

Like for detective security measures, we can say that:

$$t_d = t_d^{\,0} e^{-\alpha_d C_d} \tag{11}$$

where $t_d^{\,0}$ represents the time needed to detect without the implementation of a security measure. The function t_d is declining and convex: $\frac{\partial t_d}{\partial C_d} < 0$, $\frac{\partial^2 t_d}{\partial C_d^2} > 0$.

One of the possible security measures according to the risk-treatment options is the transfer of risk to an insurance company. In such a case the investment C presents a monthly premium, and in the case of an incident the insurance agency pays the compensation I to cover the loss.

Taking into account Equations 10 anc 11 the loss L in Equation 7 can be written as:

$$L = L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_c C_c} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \tag{12}$$

Considering the equations for the probability function intrusion ρ (9) and loss L (12), the quantitative equation for the security risk R in Equation 8 is calculated as:

$$R = T \cdot v^{\alpha_p C_p + 1} [L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_c C_c} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I] \tag{13}$$

Assessment of Investment Return and the Selection of an Optimum Measure

The decision of how to invest resources in information security is not easy and also varies from organization to organization. When determining the optimum amount of investment in information security, it is necessary to find the optimum relationship between costs and security, as shown in Exhibit 4. The costs of information security are represented by two components that are interconnected: the costs of implementing a measure (cost) and the costs of the incident (risk). The cost of a measure is the money an organization spends on an investment with which it reduces the security risk. This component increases by increasing the security of the system. The cost of the incident is the money spent by the organization after the incident happens. This component decreases by increasing the security of the system. Finding the optimum level of security that takes into account the cost of the incident and the costs of the measure is not an easy task. In order to determine the optimum level of information security, a cost-benefit analysis is often employed.

A cost-benefit analysis compares the costs of certain activities with the benefits that the activity provides. Let us assume we can assess the expected benefits and expected total costs for different levels of information-security activities. As long as the additional *benefits B* of the information-security activity outweigh the cost *C*, the introduction of security activities is reasonable.

$$B > C \tag{14}$$

The engineering manager's objective is to introduce security measures up to the point where the net benefits (i.e., benefits minus costs) are at maximum. The introduction of security measures beyond this point means that the marginal costs of the additional

security are greater than the marginal benefits. In other words, the net benefits of the introduction of security measures over the maximum point are negative. For the engineering manager it does not make any sense to spend more on the security measure than the value of the potential loss in the case of an incident.

Gordon and Loeb (2002) estimate that the optimum cost for the security measure ranges from 0% to 37% of the possible losses due to security incidents. Other researchers have extended this estimation and found situations where it is justified for the cost of the measure to be up to 100% of the possible losses (Willemson, 2006). These findings have also been successfully proven with empirical research (Tanaka, Sudoh, and Matsuura, 2005; Tanaka, Liu, and Matsuura, 2006).

The calculation of the investment cost C in information security is described in the previous section. Unlike costs, which can be obtained quite easily, it is more difficult to identify, evaluate, or measure the benefits. Security measures (e.g., firewall, antivirus, and IDS systems) themselves do not bring about direct financial benefits that can be measured.

In general, the benefits of investing in information security are viewed as cost savings by reducing the probability of an incident or reducing the consequences of security incidents; however, these benefits are normally very hard to predict accurately. The biggest problem is that it is an assessment of the cost savings related to potential events that have not yet occurred. The more successful information security is, the harder it is to see the tangible benefits. The security-measure investment benefits B are equal to the risk reduction due to the implementation of a security measure. This can be written as the difference between the risk levels before the introduction of the measure R_0 and the value of the risk after introducing the security measure $R(C)$:

$$B = R_0 - R(C) \tag{15}$$

The assessment of the economic impact of a certain measure can be analyzed with the following economic indicators: Return on Investment (ROI), Net Present Value (NPV), and Internal Rate of Return (IRR).

Return on Investment (ROI) simply defines how much an organization gets from the amount of money spent; therefore, ROI can help engineering managers decide which of the possible options gives the most value for the money invested. ROI compares the investment benefits B and the investment cost C. The result is the investment profitability expressed in percentages, where a positive ROI value means that an investment is economically justified.

$$ROI = \frac{B - C}{C} \tag{16}$$

An example illustrates the calculation: the assessed risk of the threat of a virus infection on a web server is €8,750, and after the purchase and implementation of €1,600 worth of antivirus safeguard, the reduced risk is valued at €3,400. The annual cost of maintenance and operation of the measure is €450, so the ROI in the first year is:

$$ROI = \frac{€8.750 - €3.400 - €1.600 - €450}{€1.600 + €450} = 160\% \tag{17}$$

The ROI calculation can be shown for the different security measures that are presented above. For different security measures, the appropriate adjustments to the risk Equation 13 are required. If the selected risk-reduction strategy is an investment into a *preventive security measure* s_p, which reduces the vulnerability of the asset, the ROI Equation 16 is written as:

$$ROI = \frac{T \cdot v\,(1 - v^{\alpha_p C_p}) \cdot L - C_p}{C_p} \tag{18}$$

If the selected risk-reduction measure is an investment into a *corrective security measure* s_c, which reduces the loss, then the ROI Equation 16 has the following form:

$$ROI = \frac{TvL_1 t_r^{0}\,(1 - e^{-\alpha_c C_c}) - C_c}{C_c} \tag{19}$$

Transfer of risk to an insurance company represents a corrective security measure, because the transfer of risk to an insurance company does not reduce the incident probability—it only mitigates the consequences of an incident. Equation 16 can be expressed as follows:

$$ROI = \frac{TvI - C}{C} \tag{20}$$

While ROI tells us what percentage of return will be provided with the investment over a specified period of time, it does not tell us 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?

In the case of long-term investments, the time attribute represents a problem when calculating the ROI, and managers generally use the financial metric *Net Present Value (NVP)* when comparing benefits and costs over different time periods. The methodology behind NPV is in discounting all the anticipated benefits and costs to today's value, where all the benefits and costs are expressed in a monetary unit (e.g., euros):

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} \tag{21}$$

In Equation 21, i represents the discount rate and n represents the period of time. The discount rate i is generally understood as the average cost of capital. The selection of the appropriate discount-rate value to calculate the NPV indicator is very important. NPV controls the risk via the discount-rate value: a higher discount rate means a lower value of NPV. The NPV is measured in monetary terms, while an investment is economically justified when the NPV is equal to or greater than zero. The essence of the NPV approach is to compare the discounted cash flows associated with the future benefits and future costs to the initial investment costs. For the ease of calculation, it is often assumed that the future benefits and costs, with the exception of the initial investment cost, are realized at the end of the time period.

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 an annual €5,000 for three years. Both solutions cost €15,000, but the second solution is better because the 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.

Internal return rate IRR makes it possible to find the discount rate at which the NPV equals zero, or in other words, IRR sets the discount rate at which the present value of inflows equals the present level of outflows.

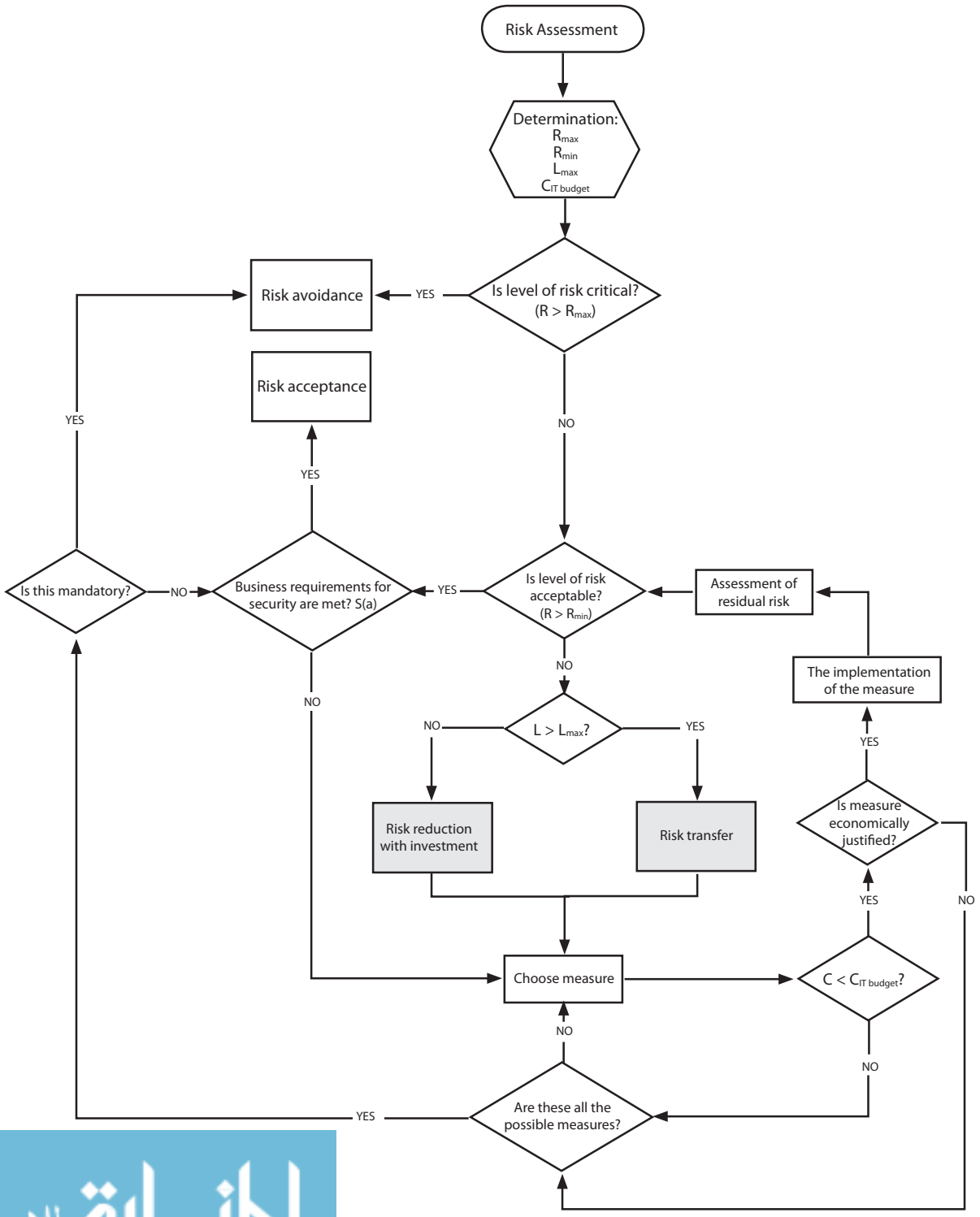
$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1 + IRR)^t} = 0 \tag{22}$$

In the search for an optimum security measure from the economic point of view, it is advisable to consider the security solution with the highest ROI, NPV, and IRR; however, this is sometimes difficult to achieve since it could happen that the ROI is in favour of one of the solutions, the NPV of another, and the IRR of a third one. In such cases, other parameters have to be considered and a decision has to be made on subjective terms. Although the ROI has some weaknesses compared to the NPV and the IRR, the ROI is still the most popular indicator in practice. According to a CSI survey (2011), 54% respondents used the ROI, 22% used the NPV, and 17% used the IRR.

Risk-Management Process

The overall process of security-risk management is presented in Exhibit 5. The process starts with the selection of the risk-limit parameters R_{min}, R_{max} and L_{max} and proceeds with the risk assessment. The selection of the security measure is based on a risk treatment. The security-measure selection depends on the corporate budget for information-security investments C_{IT_budget}, where the cost of an individual measure C must not exceed the budget. In the case that the risk-reduction process does not provide any suitable measure to counteract a specific risk, then the strategy should be re-estimated, either by allowing risk acceptance or by implementing the avoidance strategy.

Exhibit 5. Risk-Management Process



Case Study

The examples used to illustrate the model application in real-life circumstances were prepared in cooperation with a company working in the area of IT. These examples were used to test the adequacy of the model in a real business environment. Different threats were selected, including threats such as viruses, spam, phishing, unauthorized web-page content alteration, and information-service failure. Here we present examples involving phishing and web-page content alternation. The company selected the following limit value for the risk parameters:

- Maximum risk R_{max} = €725,000/year
- Maximum loss L_{max} = €2,900,000
- Minimum risk R_{min} = €23.4/year

Example 1: Risk Analysis of Unauthorized Changes to Website Content

The vulnerability of an application entails various incursions, such as SQL injection or cross-site-scripting, by way of which a malicious user may alter the content of a public website. Nevertheless, the vulnerability of online applications is relatively small due to the appropriate development of these applications. The following security parameters were taken:

- $v = 0.05$
- $T = 2.73*10^{-3}$/day
- $\rho = 1.36*10^{-4}$/day
- $t_r^0 = 8$ hours
- $t_d^0 = 8$ hours
- L_1 = €93.6/hour
- L_2 = €0/hour
- L_3 = €8000
- L = €8093.6

Security risk is thus estimated at:

- $R = \rho \cdot L = 1.365 \cdot 10^{-4}$ / day · €8093.6 = €1.1088/day = €404.71/year

The value of the risk indicates that it can be reduced by investing in the selected security measure. The assessment of the characteristics of the selected measures, productivity, and the measure costs for a period of 4 years is presented in Exhibit 6.

The evaluation of each measure is presented in Exhibit 7 and Exhibit 8. From the economic point of view, measure A is the optimum measure because it gives positive values for the ROI, NPV and IRR.

Example 2: Risk Analysis of Phishing

"Phishing" refers to misleading e-mails and websites that try to obtain a user's identity. A person with malicious intent seeks to obtain data such as passwords, credit-card numbers, and other personal data. Such a person tries to convince the users that they are providing them with personal information only. We have taken the following security parameters:

- $v = 0.1$
- $T = 2.73*10^{-4}$ /day
- $\rho = 2.73*10^{-5}$/day

Exhibit 6. Cost Assessment for Risk-Reduction Security Measures in Relation to Unauthorized Alterations of Website Contents

Measure	Purchase and Upgrade Costs (€)	Maintenance Costs (€)	α (× 10^{-3})
Measure A – website security upgrade	initial cost: € 1,223.15 annual upgrade: -	annual maintenance: -	4.09
Measure B – firewall application warding off such assaults	initial cost: € 2,470.59 annual upgrade: € 500.00	annual maintenance: € 282.35	0.65

Exhibit 7. Economic Evaluation of Risk-Reduction Security Measures in Relation to Unauthorized

		A			B		
Year	Discount Rate	Benefits (€)	Purchase and Upgrade Costs (€)	Maintenance Costs (€)	Benefits (€)	Purchase and Upgrade Costs (€)	Maintenance Costs (€)
0			1223.15			2470.59	
1	0.05	384.47	0.00	0.00	364.24	500.00	282.35
2	0.05	384.47	0.00	0.00	364.24	500.00	282.35
3	0.05	384.47	0.00	0.00	364.24	500.00	282.35
4	0.05	384.47	0.00	0.00	364.24	500.00	282.35

Exhibit 8. Calculation of ROI, NPV, and IRR Risk-Reduction Security Measures in Relation to Unauthorized Alterations of Website Content

Measure	ROI	NPV	IRR
A	26%	140.16 €	10%
B	- 74%	-3953.21 €	-

- t_r^0 = 16 hours
- t_d^0 = 0 hours
- L_1 = €23.4/hour
- L_2 = €11.7/hour
- L_3 = €1000
- L = €1376.47

Security risk is estimated at:

- $R = \rho \cdot L = 2.73 \cdot 10^{-5} / day \cdot €1376.47 = €0.0375/day = €13.71/year$

The value of the risk is such that the risk could be accepted, while another option is to reduce the risk by investing in the security measure. Assessment of the characteristics of the selected measures, productivity, and measure costs for the period of 4 years is presented in Exhibit 9.

The evaluation of each measure is presented in Exhibit 10 and Exhibit 11. Both measures give negative results for the ROI and NPV, which coincide with the fact that the risk is acceptable for the organization due to its low level. The value of risk *R* in this example is too small and does not make it possible for a security measure with a positive result to be found. For a positive ROI and NPV, the costs *C* of such a measure must be very small.

Conclusions

Information security is an area in which interest is rapidly increasing. Organizations are now more aware that security is one of the basic elements of any information system. This raises crucial questions—"How secure is the information system?" and "How secure should the information system be?" It is important that we are aware that a fully secure system does not exist. An enterprise should choose a security level that is acceptable to the organization; however, determining an appropriate security level is a challenging task, which is implemented through the process of security-risk management.

The risk-management process helps organizations decide on the necessary investments in security measures that are the most effective for the organization. The basic risk-management strategy is to reduce the risk by introducing appropriate technologies, tools, or procedures. This reduces the probability of a security incident or damage caused by the incident. Investing in measures related to information security is, therefore, inevitable for all organizations that are involved in the process of electronic commerce.

People responsible for security-related investments are wondering in which solution to invest and in particular how much to invest. This is because before investing in a particular measure it is good to know whether or not the investment is financially justified. Information security is no exception. The economic approach to managing security-risk assessment and selecting the optimum measure in information security is typically a large project. It implies a thorough analysis and evaluation of the information assets, an analysis of threats attacking information assets, an analysis of the consequences of information-technology failure, an analysis of the probability of a successful attack, and an assessment of the costs and benefits resulting from an investment in information security.

Exhibit 9. Cost Assessment for Phishing Risk-Reduction Measures

Measure	Purchase and Upgrade Costs (€)	Maintenance Costs (€)	α (× 10^{-3})
Measure A: user training and awareness	initial cost: € 2,047.06 annual upgrade: € 500.00	annual maintenance: € 141.18	0.63
Measure B: security upgrade on the proxy server	initial cost: € 2,225.59 annual upgrade: -	annual maintenance: € 282.35	1.79

Exhibit 10. Economic Evaluation of Individual Measures Aimed at Reducing Phishing Risk

		A			B		
Year	Discount Rate	Benefits (€)	Purchase and Upgrade Costs (€)	Maintenance Costs (€)	Benefits (€)	Procurement and Upgrade Costs (€)	Maintenance Costs (€)
0			2047.06			2225.59	
1	0.05	10.32	500.00	141.18	13.08	0.00	282.35
2	0.05	10.32	500.00	141.18	13.08	0.00	282.35
3	0.05	10.32	500.00	141.18	13.08	0.00	282.35
4	0.05	10.32	500.00	141.18	13.08	0.00	282.35

Exhibit 11. Calculation of ROI, NPV, and IRR Risk-Reduction Measures for Phishing

Measure	ROI	NPV	IRR
A	- 99%	- 4284.03 €	-
B	- 98%	- 3180.43 €	-

This article presents a comprehensive model for managing information-security risks that allows an evaluation of the investments in security and the protection of business-information systems. The model is based on a quantitative analysis of security risks and allows an evaluation of different investment options in information security. The model is designed as a standard procedure that leads an organization from the initial input data selection to the final recommendations for the selection of an optimum measure that reduces a certain security risk.

The biggest advantage of the model is that it allows a direct comparison and a quantitative evaluation of the various security measures: technological security solutions, the introduction of organizational procedures, training, or the transfer of risk to an external company. The output data of the model is the profitability of each security measure as measured by the ROI, NPV, and IRR, and a comparison of individual measures. In the process of evaluating the optimum level of an investment in information security, it is necessary to quantitatively evaluate the vulnerabilities and threats that are related to an information asset as well as measures to reduce these risks. A quantitative evaluation of these parameters is the basis for assessing the economic viability of individual investments using the indicators ROI, NPV, and IRR. The model was tested and applied in practice to a real company, which confirms the correctness and effectiveness of the model; however, the model results are very dependent on the accuracy of the data input. Some threats are still lacking good historical data on which the input data can be precisely determined. We expect that in the future increasing amounts of historical data will be available, which will positively influence the use of quantitative approaches.

References

Acquisti, Alessandro, Allan Friedmanm, and Rahul Telang, "Is There a Cost to Privacy Breaches? An Event Atudy," *Proceedings of the International Conference of Information Systems ICIS* (2006).

Anderson, Ross, "Why Information Security Is Hard – An Economic Perspective," *Proceedings of the 17th Annual Conference*, ACSA 2001 Computer Security Applications (2001), pp. 358-365.

Anderson, Ross, and Bruce Schneier, "Economics of Information Security," *IEEE Security and Privacy, 3*:1 (2005), pp. 12-13.

Arora, Ashish, and Rahul Telang, "Economics of Software Vulnerability Disclosure," *IEEE Security and Privacy, 3*:1 (2005), pp. 20-25.

Baryshnikov, Yuliy, "IT Security Investment and Gordon-Loeb's 1/e Rule," *Proceedings of the 11th Workshop on the Economics of Information Security (WEIS 2012)*, Berlin, Germany (2012).

Bojanc, Rok, and Borka Jerman-Blažič, "An Economic Modelling Approach to Information Security Risk Management." *International Journal of Information Management, 28*:5 (2008), pp. 413-422.

Bojanc, Rok, Borka Jerman-Blažič, and Metka Tekavčič, "Managing the Investment in Information Security Technology by Use of Quantitative Modeling Approach," *Information Processing & Management*, *48*:6 (2012), pp. 1031-1052.

Bahill, Terry A., and Eric D. Smith, "An Industry Standard Risk Analysis Technique," *Engineering Management Journal, 21*:4 (2009), pp. 16-29.

Cavusoglu, Huseyin, "Economics of IT Security Management," *Economics Of Information Security, 12* (2004), pp. 71-83.

Computer Security Institute (CSI), "2010/2011 Computer Crime and Security Survey," *The 15th Annual Computer Crime and Security Survey*, Computer Security Institute (2011).

Farahmand, Fariborz, Shamkant B. Navathe, Gunter P. Sharp, and Philip H. Enslow, "Managing Vulnerabilities of Information Systems to Security Incidents," *Proceedings of the 5th International Conference,* Electronic Commerce (2003), pp. 348-354.

Geer, Dan, *Security of Information When Economics Matters*, Verdasys (2004).

Gordon, Lawrence A., and Martin P. Loeb, "The Economics of Information Security Investment," *ACM, 5*:4 (2002), pp. 438-457.

Gordon, Lawrence A., and Martin P. Loeb, "Using Information Security as a Response to Competitor Analysis Systems," *ACM*, *44*:9 (2001), pp. 70-75.

Gordon, Lawrence A., and Martin P. Loeb, *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw Hill (2005).

Gordon, Lawrence A., and Robert Richardson, "The New Economics of Information Security," *Information Week, 53-56* (April 13, 2004).

ISO/IEC 15408, "Information Technology - Security Techniques - Evaluation Criteria for IT Security," *International Organization for Standardization* (2008).

ISO/IEC 27000, "Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary," *International Organization for Standardization* (2009).

ISO/IEC 27005, "Information Technology - Security Techniques - Information Security Risk Management," *International Organization for Standardization* (2008).

ISO/IEC Guide 73, "Risk Management - Vocabulary," *International Organization for Standardization* (2009).

Kaplan, Ray, "A Matter of Trust," *Information Security Management Handbook, 6th Ed.*, Auerbach Publications (2007), pp. 295-310.

Matsuura, Kanta, "Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model," *Workshop on the Economics of Information Security (WEIS 2008)*, (2008).

McGraw, Gary, *Software Security: Building Security In*, Addison-Wesley (2006).

NIST, "Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook," *National Institute of Standards and Technology* (2005).

NIST, "Special Publication 800-60 Workshops, Mapping Types of Information and Information Systems to Security Categories," *National Institute of Standards and Technology* (2004).

Pinto, Ariel C., Ashish Arora, Dennis Hall, and Edward Schmitz, "Challenges to Sustainable Risk Management: Case Example in Information Network Security," *Engineering Management Journal*, *18*:1 (2006), pp. 17-23.

Ryan, Julie J.C.H., and Daniel J. Ryan, "Expected Benefits of Information Security Investments," *Computers & Security, 25*:1 (2006), pp. 579-588.

Sandhu, Ravi, "Good-Enough Sercurity: Toward a Pragmatic Business-Driven Discipline," *IEEE Internet Computing, 5*:3 (2003), pp. 66-68.

Schneier, Bruce, *Beyond Fear: Think Sensibly about Security in an Uncertain World*, Copernicus Books (2003).

Schneier, Bruce, *Secrets & Lies, Digital Security in a Networked World*, Wiley Publishing (2004).

Soo Hoo, Kevin J., "How Much Is Enough? A Risk-Management Approach To Computer Security," *Stanford University* (August 2000).

Tanaka, Hideyuki, Wei Liu, and Kanta Matsuura, "An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan," *Workshop on the Economics of Information Security (WEIS 2006)*, (2006).

Tanaka, Hideyuki, Kanta Matsuura, and Osamu Sudoh, "Vulnerability and Information Security Investment: An Empirical Analysis of e-Local Government in Japan," *Journal of Accounting and Public Policy, 24*:1 (2005), pp. 37-59.

Willemson, Jan, "On the Gordon and Loeb Model for Information Security Investment," *Workshop on the Economics of Information Security (WEIS 2006)*, (2006).

About the Authors

Rok Bojanc, PhD, obtained his PhD in the field of Management Information Science from the University of Ljubljana. He works as an IT Manager at ZZI, a software solution company active in e-business exchange area. As both a technical lead and project manager, he has worked in designing, developing, implementing, and managing information systems. He has written many handbooks, technical articles, and training courses for subjects including IT, networks, security, and information systems.

Borka Jerman-Blažič, PhD, is a full professor at the University of Ljubljana and heads the Laboratory for Open Systems and Networks at Jožef Stefan Institute. She holds an MS in electrical engineering from the University of Ljubljana and a PhD in natural and computing sciences from the University of Zagreb. Currently Dr. Jerman-Blažič works as an advisor to the Information Security Unite of Stockholm University, Department of Systems and Computer Science.

Contact: Rok Bojanc, ZZI, Pot k sejmišču 33, Ljubljana, Slovenia; phone: +38601530330; rok@bojanc.com