DOI: 10.2478/v10051-012-0027-z

Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System

Rok Bojanc[1], Borka Jerman-Blažič[2]

[1]ZZI, Pot k sejmišču 33, 1231 Ljubljana-Črnuče, Slovenia, rok@bojanc.com
[2]Jožef Stefan Institute, Jamova 39, 1000 Ljubljana, Slovenia, borka@e5.ijs.si

The paper presents a mathematical model for the optimal security-technology investment evaluation and decision-making processes based on the quantitative analysis of security risks and digital asset assessments in an enterprise. The model makes use of the quantitative analysis of different security measures that counteract individual risks by identifying the information system processes in an enterprise and the potential threats. The model comprises the target security levels for all identified business processes and the probability of a security accident together with the possible loss the enterprise may suffer. The selection of security technology is based on the efficiency of selected security measures. Economic metrics are applied for the efficiency assessment and comparative analysis of different protection technologies. Unlike the existing models for evaluation of the security investment, the proposed model allows direct comparison and quantitative assessment of different security measures. The model allows deep analyses and computations providing quantitative assessments of different options for investments, which translate into recommendations facilitating the selection of the best solution and the decision-making thereof. The model was tested using empirical examples with data from real business environment.

Keywords: Modelling, Security Technology, Economic metrics, Investment, Enterprise Information System

1 Introduction

The Internet is a public space in which reliability and safety of e-business and e-commerce operations is guaranteed by the infrastructure security for operators, and the software and data security for the authorized users and owners. As a consequence, the individual, corporate and government assets are taking an increasingly dematerialized form, as the storage of digital data is becoming equivalent to the productivity gains in all respects. The volume of data and information doubles each year, while the value of the corporate and government assets is increasingly derived from or encapsulated in this digital, cultural and industrial asset base. Introduction of the concept of digital assets opened up a rift with much wider implications than those of the general information management; namely, it includes the intellectual property rights management (IPR), digital rights management (DRM), copyrights and online sharing of information.

A significant portion of new companies own almost exclusively intangible industrial assets (databases, computing programs, manufacturing processes, logistic process design, other business secrets, and IPR assets), which are overtaking in importance the real estate and other tangible assets. The security objectives related to the digital-asset base are expressed in terms of confidentiality (non-disclosure to unauthorized persons), integrity (non-alternation of content), and availability (the ability of authorized users to access and use these assets without being hindered by unintentional or malicious acts). Despite the architectures deployed to ensure greater reliability and service connectivity, and despite the anti-piracy measures undertaken to protect sensitive data, it is clear that computer systems regularly fail or are subject to malicious attacks.

Architectural security of the Internet network and data security (software and data) still present the key challenges for the future Internet design. The digital world is open to all, which means that security has to be provided by the underlying architecture; nevertheless, the socio-economic environment needs to be taken in account as well.

Almost a decade ago, a number of researchers began to realize that information security is not a problem that could be resolved by technology alone; thus, they tried to include

Received: 23rd May 2012; revised 10th September 2012; accepted 15th October 2012

the economic point of view into the equation. This approach enables business managers to develop better understanding of security investments, because technical analysis of 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).

When looking at the information security system from the economics point of view, many answers can be found to the questions where strictly technical explanations fail to give satisfying answers (Gordon and Loeb, 2002). How to provide security for the IT-based operations? Which security level is adequate? How much money should be invested in security? Companies mainly seek answers to these questions in the framework of risk management.

Information security risk management is the overall process which integrates identification and analysis of risks to which an organization is exposed, assessment of the potential impact on the business, and decision regarding the action to be taken 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, consequences of security incidents, and likelihood of successful attacks on the systems exposed to the digital world, as well the cost and benefit analysis of the security investments (Hoo, 2000). Risk management process typically consists of two main stages known as risk assessment and risk treatment. Risk assessment is the process of deciding whether existing protection is sufficient to protect information assets against possible threats. The assessment provides information about the threats to which organization assets are exposed and information system vulnerabilities that could be abused by the threats. Risk treatment is a process of selection and implementation of security measures to reduce risk. The treatment usually consists of risk avoidance, risk mitigation, risk transfer and risk acceptance. Standards and guidelines are available for the information security management, such as the ISO 27000 series and NIST publications (ISO, 2005). However, the advancements in the field of technology require more sophisticated decision-making approaches when it comes to for the security technology investments, and data and digital asset protection (Gordon and Richardson, 2004).

This paper presents a mathematical model for the security technology investment evaluation and optimal decision-making, based on the quantitative analysis of the security risks and digital asset assessments. The novelty of the model is in the use of the results of a quantitative analysis of different security measures that counteract individual risks within the information processing in a particular organization. The risk is identified with the analysis of the potential threats. The selection of security technology is based on the efficiency of the security measures and the related cost. Economic indicators are used for the efficiency assessment of the measures. Measures are compared and most appropriate protection technology is selected. The model is presented as a procedure that provides overall assessment of all possible security measures that reduce the risk in a particular organization with identified vulnerabilities in the information processing, related asset values and the available protection technology. The advantage of the model is in the completeness of the considered security measures that encompasses not only the protection technology but also organizational approaches, insurance possibilities or outsourcing solutions. The model provides good guide lance for practical use. The usability of the model is illustrated with several examples of possible security incidents and the selected measures.

2 Related research

Information security was traditionally considered as a technical discipline, whose purpose was to provide the maximum level of security (McGraw, 2006). In the last decade, a major economic component was considered in the related research as investments in information security are rapidly increasing (Anderson, 2001). Information security economics, a relatively new field of study, uses economic theory and models (Bojanc and Jerman-Blažič, 2007) to analyse 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 quantification of 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. Estimation of the total cost of security breaches can be done in several ways. Some approaches try to quantify short-term and long-term costs, or tangible and intangible costs, while other methods use the market efficiency theory and 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 the accident is just an approximate value of the true cost of the security breach (Farahmand, 2003). Farahmand (2003) suggest 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 the qualitative approach to obtain quantitative probability estimates.

Calculation of optimal investment in information security is relatively new approach in the area of enterprise information technology. The focus regarding IT security solutions was previously oriented exclusively on search of technical tools and methods, without any consideration of the financial costs. In the last ten years few approaches for solving the problem were proposed. The proposed analytical models are based on a cost-benefit analysis. The potential risk of security incidents is considered in relation to the likelihood they to happen and the potential damage. One of the first analytical decision-making

frameworks for evaluating different IT security policies was proposed by Hoo (2000). In his work he is replicating the group of protective measures or policies, and for each policy is trying to find the best compromise between costs and benefits. Gordon and Loeb (2001) propose an economic model that determines the optimal 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) 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 the expected-loss-risk measurements. The approach to base their investment decision on 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 available data are censored and therefore biased, the quality of 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 scenario. Based on these findings, Bojanc, Jerman-Blažič and Tekavčič (2012) presented a general mathematical model for quantitative evaluation of investments in a variety of security measures and the selection of the optimal security solutions. An alternative method uses the so-called game theory (Cavusoglu, 2004). Cavusoglu argues that the traditional decision-analytic approaches to evaluating IT security investments treat the security technology as a black box and do not consider the difference between the investments in information security solutions from general IT investments. He is treating the information security as a game between organization and the potential attackers with a motive to cause damage for personal profit or satisfaction. 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 touchpoints (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. The past breaches of information security have resulted in both immediate and indirect losses. Indirect losses have often been more serious than the direct ones. The optimal level of information security investments is treated on the basis of the expected cost/benefit investment trade-offs.

In this work we focus on the more exact quantification of the security risks and on the digital asset assessments required for optimal selection of the security technology investment. The security measures that counteract individual risks are quantified in the context of their application within the information processes that take place within an organization. The target security levels for all identified business processes are quantified, as well as the probability of a security accident together with the expected loss. The model is applied on several examples of possible security incidents and illustrated with the results based on simulations.

3 Quantitative risk assessment

The objective of risk assessment is the identification and measurement of risk in order to obtain relevant information for decision-making process. Risk assessment requires information about the information assets within an organization, the threats to which assets are exposed and system vulnerabilities that threats could abused. The model is based on *business processes P* that are supported by *information assets a*. The risk assessment procedure determines and evaluates the vulnerabilities and the threats for every information asset. The risk assessment output data is the *security risk R* defined as a product of the estimated probability of occurrence of a security incident ρ and the loss due to a security incident L:

$$R = \rho \cdot L \tag{1}$$

Information security incident is defined as single event or a series of unwanted or unexpected information security events with a probability of compromising the business operations. There are different kinds of security incidents. Some incidents result in abuse of confidentiality, such as the disclosure of bank accounts. Incidents can also related in abuse of integrity, such as malicious deletion or modification of the business data. Other incidents may abuse the service availability and they are known as Denial-of-Service (DoS) attacks. *Probability of a security incident occurrence* ρ ($0 \leq \rho \leq 1$) depends on the probability T of a threat occurring, and the vulnerability v, defined in the model as the probability that a threat once realized (i.e., an attack) would be successful (Gordon and Loeb, 2002).

$$\rho = T \cdot v \tag{2}$$

Threat can be defined as a potential cause of undesired incidents that may cause damage to the system or organization (ISO 27000, 2009). *Threat probability* T ($0 \leq T \leq 1$) is defined as a probability of an attack occurrence on information assets. Some of threats can be successful, resulting in a security incident, while others are not successful. The potential for a success is measured with the probability parameter.

Information assets have vulnerabilities that threats could exploit. Vulnerability can be defined as a 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 a

theft. 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. In our model the *vulnerability* v ($0 \le v \le 1$) is defined as the probability a threat to be successfully realized as incident on an information asset. The effectiveness of threat is determined with the level of the vulnerability of an information asset. Limit value $v=0$ indicates that the information assets are completely protected and secured, while $v=1$ means the information assets are totally vulnerable.

Function ρ in equation (2) fulfils two basic boundary conditions. Incident probability has zero value when there are no attacks (attack probability is zero), and probability of a security incident is zero when the system is free of vulnerabilities (vulnerability is zero).

In case of a security incident, an organization suffers *financial loss L*. The loss $L>0$ is measured in monetary units (e.g., in euro). The true financial loss of a security incident is difficult to assess. It is relatively easy to calculate the immediate direct loss due to an incident. This represents losses of revenue, losses of productivity and increased costs. Much more difficult is assessment of 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, financial market, banks and business alliance relationships. The quantitative evaluation of loss can be supported through the allocation of losses to individual factors and separately calculate the loss of each factor:

$$L = L_s + L_r(t) + L_i(t) + L_p(t) + L_{SLA} + L_{indirect} \qquad (3)$$

Detailed definitions and mathematical derivation of the individual factors in equation (3) is explained in details in Bojanc, Jerman-Blažič and Tekavčič (2012).

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

Cost of repair works $L_r(t)$ is the price of repair works of employees or external contractors, to eliminate the consequences of the security incident and restore system or service in normal operation

Corporate *income loss* $L_i(t)$ represents the loss suffered on the revenue side due to 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 their customers a particular service according signed in the Service Level Agreement (SLA) contract. In cases when the availability of offered services are 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 potentially long-term consequences represent damage to the reputation of the organization, the interruption of business processes, loss of intellectual property, and damage to customer confidence.

Security incident can cause downtime of the information system or services. Downtime consists from the *time to detect* t_d a security incident and *time to repair* t_r information system and restore the functionalities of a system. Time t_d is accounted for from the moment of an incident occurrence to the moment of the incident detection.

The equation (3) can be simplified by grouping the items in three factors. The first factor depends on t_r, the second factor depends on t_d and third factor which is not time dependent (Bojanc, Jerman-Blažič and Tekavčič, 2012). Individual factors in the equation (3) may contain either t_r, t_d or both. The factors L_r, L_p and L_i contain time parameter t_r, the factors L_i and L_p contain time parameter t_d, while factors L_s, L_{SLA} and $L_{indirect}$ have no time dependence. Considering that, the equation (3) can be rewritten by taking in account the dependence of the time parameter t_r and t_d:

$$L = L_1^{'} \cdot t_r + L_2^{'} \cdot t_d + L_3 \qquad (4)$$

Factor L_1' includes data on the L_r, L_i and L_p, factor L_2´ includes data on the L_i and L_p and factor L_3 includes data on the L_s, and L_{SLA} and $L_{indirect}$. Factor L_3 is expressed in monetary units (e.g. the Euro), the factor L_1´ and L_2´ are expressed in monetary units per unit time (e.g. Euro / hour).

Taking into account the financial loss in equation (4) and the likelihood of an incident in equation (2) the security risk R from equation (1) may be specified as presented in equation (4).

$$R = T \cdot v \cdot \left[L_1^{'} \cdot t_r + L_2^{'} \cdot t_d + L_3 \right] \qquad (5)$$

The security risk R represents the expected financial loss caused by the security incident measured in the same monetary unit as L (e.g., in Euro).

4 Determination the risk treatment

There are multiple strategies available to treat each security risk. On the basis of risk assessment the organization can select one of the possible options, such as:

- *Reduction* of security risk by implementing an appropriate technologies and tools (such as firewall, antivirus systems etc.) or adopting appropriate security policies (like passwords, strong authentication tools, access control, port blocking etc.). This reduces the probability of security incident or limits the loss in case the incident happens. Reduction is primary risk management strategy.
- *Transfer* of security risk to either outsourcing security service provision bodies or insurance agency. This way of transferring the risk recently has become important strategy in provision of security measures within the organization.
- *Avoidance* of security risk 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 type of assets such as full open connectivity to Internet. When engineering manager selects risk avoid-

ance, organization terminates some of its activities on the network or protects them against risk.
- *Acceptance* of security risk as a part of business operations. Risk acceptance 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.

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. Combination of several measures is also an option; e.g. an organization first reduces 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.

Selection of appropriate risk treatment can be presented on the risk treatment diagram as probability of the incident and losses due to an incident. This is presented in Figure 1. The curves on this diagram represent the points with the same risk value. 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 incident ρ, the risk point is moving vertically downward from point R_0 to 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 R_2.

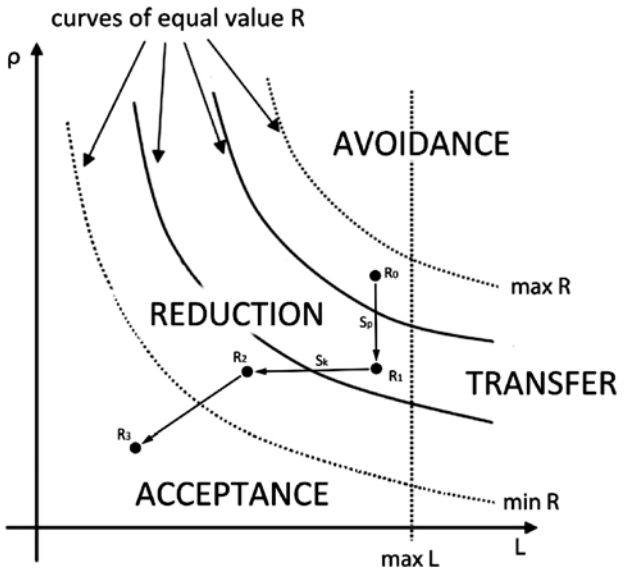

Figure 1: Risk treatment determination

Each of this risk treatment option represents certain area on the graph. It is necessary to define a *risk parameter limit values* which present the three border lines dividing area in the graph into four units, where each area correspond to a specific risk treatment option (Bojanc and Jerman-Blažič, 2008). Risk limit values are specified as follows:
- R_{max} – maximum risk value still acceptable for the organization
- L_{max} – maximum one-time loss still acceptable for the organization
- R_{min} – minimum risk value still plausible for the organization

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 negligible low, so the implementation of a security measure is not financial justified and risk is accepted. The second border line is the maximum risk value ($R>R_{max}$) above which the risk is avoided. The third boundary line is the maximum single loss ($L>L_{max}$) due the incident. Schneier (2003, p. 23) goes as far as saying that serious consequences, regardless of their low frequency of occurrence, are not acceptable. Above this value the risk impact can have catastrophic consequences and recommended risk treatment option for this area is a transferring the risk. Security risk in the rest area ($L<L_{max}$) is treated by reducing risk through the investment in security measures.

5 Security measure selection

Security measures are activities, procedures or mechanisms to prevent or reduce damage caused by the realization of one or more threat. Security measures may be physical protection, diagnostic sensors, alert devices, software solutions for protection, organization policies and procedures. Many of the measures include detection, deterrence, prevention, mitigation, repair, recovery, control and awareness. Appropriate selection of security measures is essential to effective information security. Figure 2 shows how the organization protects itself against potential security attacks by implementing *security measures* that can be classified into three categories according to their impact on the risk parameters R, ρ and L:
- *Preventive security measures* s_p, which reduce the probability of a security incident ρ (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 needed for an incident detection t_d, and enable the threat information gathering (e.g., IDS systems).

The introduction of preventive measure s_p (at Figure 1) shifts the risk point on the graph vertically downwards (from R_0 to R_1) to a lower risk curve. The corrective security measures are different from the preventive security measures reducing the incident probability as they act towards the reduction of the loss in case of a successful incident. The introduction of corrective measures s_c and detection measures s_d move the risk point horizontally on the graph to the left of 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. In case an incident is not detected by detective security controls, it can be identified through the consequences and from other footprints left behind by the malicious user or malicious code. The use of detective protection enables loss reduction and a more realistic assessment of attack probability T, and incident probability ρ. When companies are not using detective controls, the probability values

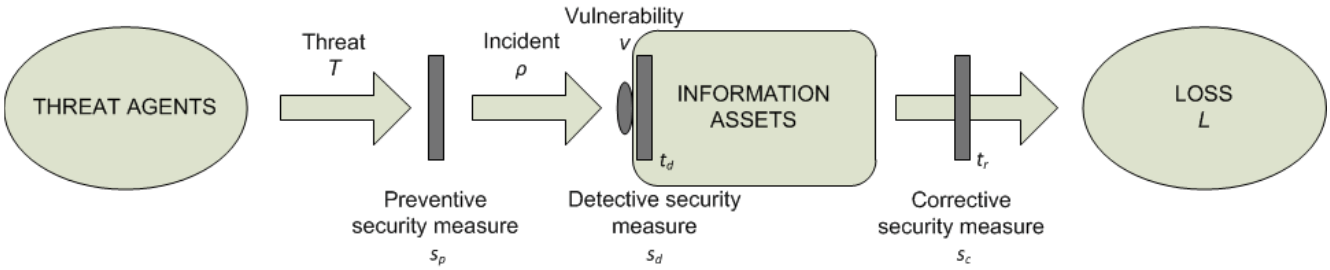

Figure 2: Integrating security measures into the model

are merely an estimate and they can differ much from realistic values. Wrong assumptions can also lead to non-optimal selection of security measures.

5.1 Security measure quantification

Each *security measure* $s(\alpha, C)$ is defined by two quantitative parameters productivity of measure α and cost of measure C. *Security measure productivity* $\alpha(t) > 0$ presents the impact of a security measure on the risk reduction. *Cost of measure C* is defined as an investment expressed in some currency (e.g., in euro). This takes in account all expenses related to the implementation of the selected security measure, expenditure in capital investment and operational costs. An example of capital investment is purchase of a new system for intrusion detection in the network, which reduce the likelihood of security intrusions in particular time period in the organizational network. Operational costs are one-time cost of implementation, testing and training, the cost of fixes and upgrades, maintenance cost and other expenses related to the introduction of a measure.

When introducing the 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 ($0 \leq C \leq C_{IT\_budget}$). If the cost of a measure is higher the implementation of the measure is not possible. A CSI research has shown that almost half of the companies spends more than 6% overall budget resources for IT security (CSI, 2011).

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

5.2 Security risk reduction

Security measures $s(\alpha, C)$ reduce security risk R. The introduction of preventive security measure $s_p(\alpha_p, C_p)$ reduces security incident probability ρ. Function ρ in equation (2) is supplemented in a way that introduces dependency from the *preventive security measure* investment C_p. Various incident probability ρ functions are available (Matsuura, 2009; Gordon and Loeb, 2002). In the presented model we used:

$$\rho(T, v, C_p) = T \cdot v^{\alpha_p C_p + 1} \tag{6}$$

This function fits the boundary condition that in case of an unlimited investment, the incident probability limits towards zero:

$$\lim_{C_p \to \infty} \rho(T, v, C_p) = 0 \tag{7}$$

Preventive security measure s_p reduces the incident probability; this can be described as:

$$\frac{\partial \rho}{\partial C_p} < 0, \frac{\partial^2 \rho}{\partial C_p^2} > 0 \tag{8}$$

Corrective security measures $s_c(\alpha_c, C_c)$ reduces the time to repair, consequently reducing the organization's loss caused by the incident. This is expressed by the following equation:

$$t_r = t_r^0 e^{-\alpha_c C_c} \tag{9}$$

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 throughout the interval $0 \leq C_c < C_{ITsec\_budget}$:

$$\frac{\partial t_r}{\partial C_c} < 0, \frac{\partial^2 t_r}{\partial C_c^2} > 0 \tag{10}$$

As for *detective security measures* $s_d(\alpha_d, C_d)$**,** we can say that:

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

Function t_d is declining and convex throughout the interval $0 \leq C_d < C_{ITsec\_budget}$:

$$\frac{\partial t_d}{\partial C_d} < 0, \frac{\partial^2 t_d}{\partial C_d^2} > 0 \tag{12}$$

One of the possible security measures according to the risk treatment options in chapter 4 is also the *transfer of risk to an insurance company*. In such a case, investment C represents a monthly premium; in case of an incident, the insurance agency pays a compensation I to cover the loss. Since the risk transfer only reduces the loss in the event of an incident, and has no impact on the incident probability, this is considered a

special type of a corrective security measure, which is dealt with differently. $I(C) \geq 0$ parameter is added to the equation (4); this parameter represents the compensation received by the company in case of an incident. In cases where companies decide to invest into security measures other than insurance, then $I = 0$. Losses upon the occurrence of a security incident can be written as:

$$L = L_1^{'} \cdot t_r + L_2^{'} \cdot t_d + L_3 - I \tag{13}$$

Taking into account equations (9) and (11), losses incurred due to a security incident in equation (13) can be written down as:

$$L = L_1^{'} \cdot t_r^{\,0} \cdot e^{-\alpha_c C_c} + L_2^{'} \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \tag{14}$$

Cloud and hosting services is another example of the risk transfer; in case of using cloud or hosting services an organization transfers its information system (or part of its system) to the provider. In this case, the equation (3) simplifies to $L_s = 0$ and $L_r = 0$, since an organization does not invest into its own equipment. However an organization should sign an SLA with the provider, which stipulates that an organization is entitled to the compensation in case of an incident, then $I \geq 0$.

By taking in account the equations for the probability function intrusion ρ (6) and loss L (14), and the quantitative equation for security risk R from equation (5) the total risk can be now calculated as follows:

$$R = T \cdot v^{\alpha_p C_p + 1} \left[L_1^{'} \cdot t_r^{\,0} \cdot e^{-\alpha_c C_c} + L_2^{'} \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \right] \tag{15}$$

6 Return on security investment

For the assessment of economic impact of a certain security measure can be analysed with the economic indicators Return on Investment (ROI), Net Present Value (NPV), and Internal Rate of Return (IRR) which are the most often used security metrics in practice (CSI, 2011).

Return on investment (ROI) is popular accounting metric for comparison of business investments. ROI simply defines how much organization gets from the spent amount of money. Therefore ROI can help organization to decide which of the possible options gives the most value for money invested. ROI compares the investment *benefits B* and *investment cost C*. The result is investment profitability expressed in percentages; positive ROI value means that an investment is economically justified.

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

Calculation of investment cost C in information security is described in the previous section. Unlike the cost of security measure C which shall be determined relatively easily it is much harder to identify, evaluate or measure the benefits (Hoo, 2000). Security measures (e.g. firewall, antivirus and IDS systems) itself do not bring direct financial benefits that can be measured.

In general, the benefits of investment in information security are viewed as a cost savings by reducing the probability of an incident or reducing the consequences of security incidents. These benefits are normally very hard to predict accurately. The biggest problem is because it is an assessment of the cost savings related to potential events that have not yet occurred. The more successful information security is harder is to see 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 risk levels before the introduction of the measure R_0 in equation (5) and the value of risk after introducing a security measure $R(C)$ in equation (15):

$$B = R_0 - R(C) \tag{17}$$

Reduced risk in equation (17) is a technical element of the benefits. Moreover, the value of the benefit is also influenced by organizational elements, therefore we add *negative consequences* δ of the security measure on business performance which decrease benefits. We expect that the higher level of security diminishes operational capacities of a system, thus impacting productivity and business performance. We also add *indirect positive effects* μ of a security measure which increase benefits in equation (17) (e.g., improved corporate image and status, references, self-esteem, interconnectivity with the existing protective elements, fulfillment of legal duties, lower insurance premium, etc.).

$$B = R_0 - R(C) - \delta + \mu \tag{18}$$

Using the equation (18) ROI in equation (16) can be written as:

$$ROI = \frac{R_0 - R(C) - \delta + \mu - C}{C} \tag{19}$$

The calculation of an example illustrates the calculation: the assessed risk of the threat of virus infection on a web server is €8.750, and after the purchase and implementation of a €1.600 worth 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:

$$ROI = \frac{€8.750 - €3.400 - €1.600 - €450}{€1.600 + €450} = 160\% \tag{20}$$

The ROI calculation may be applied for different security measures that are presented in section 5. 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 (19) gets the following form:

$$ROI_p = \frac{T \cdot v\left(1 - v^{\alpha_p C_p}\right) \cdot L - \delta + \mu - C_p}{C_p} \tag{21}$$

In this case the loss L equals the equation (4).

If the selected risk reduction measure is to invest into a *corrective security measure* s_c, which reduces the loss, then the ROI equation (19) has the following form:

$$ROI_c = \frac{TvL_1^{'} t_r^{\,0}\left(1 - e^{-\alpha_c C_c}\right) - \delta + \mu - C_c}{C_c} \tag{22}$$

If the selected risk reduction measure is an investment into a *detective security measure* s_d, the ROI equation (19) takes the following form:

$$ROI_d = \frac{TvL_2' t_d^{\,0}\left(1-e^{-\alpha_d C_d}\right)-\delta+\mu-C_d}{C_d} \quad (23)$$

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. Since the risk transfer to an insurance company does not represent an intervention within the system, it means that δ≈0. Cost *C* denotes a monthly premium paid to the insurance company. The equation (19) can be simplified as follows:

$$ROI_t = \frac{TvI+\mu-C}{C} \quad (24)$$

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, in cases when the amount of investment is taken then the decision become easier: would the organization 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 presents a problem in calculating the ROI and managers are mainly using the financial metric *Net Present Value (NPV)* 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):

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} \quad (25)$$

In equation (25) *i* present the discount rate and *n* present the period of time. Discount rate *i* is generally understood as the average cost of capital. Selection of the appropriate discount rate value to calculate NPV indicator is very important. NPV controls the risk with the discount rate value, the higher discount rate means a lower value of NPV. The NPV is measured in monetary terms, while an investment is economically justified when 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 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 may select between two security solutions where one costs €15.000 in advance, and the other costs yearly €5.000 for three years. Both solutions cost €15.000, but the second solution is better because organization can invest the remains 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 enables the findings of the discount rate at which NPV equals zero, or in other words, the discount rate at which the present value of inflows equals the present level of outflows.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^t} = 0 \quad (26)$$

In the search of an optimal security measure from the economical prospective it is certainly 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 ROI is in favour of one of the solutions, NPV of another, and IRR of a third one. In such cases other parameters have to be considered and decision has to be taken on subjective terms. Although ROI has some weaknesses compared to the NPV and IRR, ROI is still the most popular indicator in practice. According to the survey CSI (2011) 54% responders use ROI, 22% use NPV and 17% use IRR.

Another interesting result that the model offers is cost assessment for the *economical optimal investment* in security measure. For economical optimal investments, the net benefits (i.e. benefits minus costs) are at maximum. This assessment is useful when the price frame is required or when it is necessary to know how much a certain measure deviates from an optimal selection. The method for the investment cost assessment determines the biggest net benefit of a measure (difference between benefits and costs). To simplify the calculation we assume that the parameters δ and μ are linearly dependent on the cost of security measure *C*:

$$\delta = k_1 \cdot C \quad (27)$$

$$\mu = k_2 \cdot C \quad (28)$$

Since the best net benefit is looked for, the following must be true:

$$\frac{\partial(B(C)-C)}{\partial C} = 0, \quad \frac{\partial^2(B(C)-C)}{\partial C^2} < 0 \quad (29)$$

In reality, organizations must consider limitations of IT budget to assess the optimal investment in security measure. If the IT budget limit is above optimal investment, companies can invest up to an optimal level where the net benefits are at maximum. However, if the IT budget limit is below optimal investment, companies cannot invest to the optimum level, so the optimal value of the investment in this case is thus volume of IT budget. Calculations for the *preventive*, *corrective* and *detective security measures* are:

$$C_p^* = \begin{cases} \frac{1}{\alpha_p}\log_v\left[\frac{k_1-k_2+1}{\alpha_p \eta TvL\cdot\ln\frac{1}{v}}\right] & , C_p^* < C_{IT\_budget} \\ C_p^* & , C_p^* \geq C_{IT\_budget} \end{cases} \quad (30)$$

In this case the loss *L* equals the equation (4).

$$C_c^* = \begin{cases} \frac{1}{\alpha_c}\ln\left[\frac{\alpha_c \eta TvL_1' t_r^0}{k_1-k_2+1}\right] & , C_c^* < C_{IT\_budget} \\ C_c^* & , C_c^* \geq C_{IT\_budget} \end{cases} \quad (31)$$

$$C_d^* = \begin{cases} \frac{1}{\alpha_d}\ln\left[\frac{\alpha_d \eta TvL_2' t_d^0}{k_1-k_2+1}\right] & , C_d^* < C_{IT\_budget} \\ C_d^* & , C_d^* \geq C_{IT\_budget} \end{cases} \quad (32)$$

6.1 Selection the most favourable security measure from economic and business perspective

In the previous section we calculated the quantitative assessment of the return on security investments where we considered only the economic view of selecting the appropriate investment. In addition, companies have certain business security requirements for specific business processes. For example, from manager's perspective some information assets are more important than others and companies apply better security for these assets. It is therefore necessary to consider the business security requirements when comparing different security measures with each other and selecting the appropriate measure. In this way, the quantitative assessment of individual measures is properly weighted.

Business processes introduced in chapter 3 have certain business security requirements for the protection of data and other information relevant for a particular organization. *Business process P* of an organization and the associated set of *security requirements S(P)* are specified as the required confidentiality, integrity and availability of process *P*. The value of these variables represents the desired levels of security for individual business processes. Security parameters of *information assets an* engaged in a business process *P* are based on the business process security requirements.

$$S(a) = S(P) \tag{33}$$

If there is an *n* number of business processes, then each individual process is defined as a P_i ,(i=1,…,n). For the information assets engaged in more than one business process, the security requirements can appear with different target values. In this case, the highest security target value $S(P_i)$ is selected for *S(a)*.

$$S(a) = \max(S(P_1),...,S(P_n)) \tag{34}$$

This procedure sets the desired values of security requirements for every information asset. In this way, indicators ROI, NPV and IRR are properly weighted with business security requirements. This introduced the most favourable security measure from economic and business perspective, which combines the quantitative assessment of economically optimal security measure implementation and business security requirements:

$$ROI_{bus-eco} = S(a) \cdot ROI \tag{35}$$

$$NPV_{bus-eco} = S(a) \cdot NPV \tag{36}$$

$$IRR_{bus-eco} = S(a) \cdot IRR \tag{37}$$

The most favourable security measure from economic and business perspective is not intended for the financial evaluation purposes; it is intended for the comparative analysis of different security measures for different risks.

7 Model simulations

The examples used to illustrate the model application in real-life circumstances were prepared in cooperation with an organization working in the area of IT. These examples were used to test the implementation 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 the examples with phishing and web page content alternation are presented. An organization selected the following limit value for risk parameters:

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

7.1 Example No. 1: risk analysis of phishing

'Phishing' refers to misleading e-mails and websites, which are aimed at getting hold of users' identity. A person with malicious intent seeks to get hold of data such as passwords, credit card numbers, and other personal data. Such person tries to convince the users that they are providing them with personal information only. The following security parameters were taken:

- $v = 0.1$
- $T = 2.73*10^{-4}$ /day
- $\rho = 2.73*10^{-5}$/day
- t_r^0 = 16 hours
- t_{NA}^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 risk is such that the risk could be accepted, while another option is to reduce the risk by investing into the security measure. Assessment of the characteristics of the selected measures, productivity and measure costs for the period of 4 years are presented in Table 1.

The evaluation of each measure is presented in Table 2 and Table 3. Both measures give negative results for 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 enable a security measure with positive result to be found. For positive ROI and NPV the costs *C* of such measure must be very small.

7.2 Example 2: risk analysis of unauthorized changes to website contents

Vulnerability of an application entails various incursions, such as SQL injection or cross-site-scripting, by way of which a user with malicious intent may alter the contents of a public website. Nevertheless, vulnerability of online applications is

Table 1: Cost assessment for phishing risk reduction measures

Measure	Purchase and upgrade costs (€)	Maintenance costs (€)	α (× 10-3)	δ	μ
Measure A: user training and awareness	initial cost: € 2,047.06 annual upgrade: € 500.00	annual maintenance: € 141.18	0.63	0	500 €
Measure B: security upgrade on the proxy server	initial cost: € 2,225.59 annual upgrade: -	annual maintenance: € 282.35	1.79	0	0

Table 2: 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	510.32	500.00	141.18	13.08	0.00	282.35
2	0.05	510.32	500.00	141.18	13.08	0.00	282.35
3	0.05	510.32	500.00	141.18	13.08	0.00	282.35
4	0.05	510.32	500.00	141.18	13.08	0.00	282.35

Table 3: Calculation of ROI, NPV and IRR risk reduction measures for phishing

Measure	ROI	NPV	IRR
A	-56%	-2511.06 €	-
B	-98%	-3180.43 €	-

relatively slim 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
- $t_{NA}^0 = 16$ 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:

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

The value of risk is such that it can be reduced by making investments into the security measure. Assessment of characteristics of the selected measures, productivity and measure costs for a space of time of 4 years is presented in Table 4: The evaluation of each measure is presented in Table 5 and Table 6. From the economical point of view, measure A is the optimal measure because it gives positive values for ROI, NPV and IRR.

8 Conclusion

Information security is an area for which the interest among academia and real business is increasing rapidly. Organizations are increasingly 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 the information system should be?" It's important that we are aware that a fully secure system does not exist. An enterprise should choose such security level that is acceptable to the organization. Determination of appropriate security level is a challenging task, which is implemented through the process of security risk management.

Risk management process helps organizations to decide on the necessary investments in security measures that are most effective for the organization. The basic risk management strategy is to reduce the risk by the introduction of appropriate technologies, tools or procedures. This reduces the probability of security incident or damage caused by the

Table 4: 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)	δ	μ
Measure A – website security upgrade	initial cost: € 1,223.15 annual upgrade: -	annual maintenance: -	4.09	0	0
Measure B – firewall application warding off such assaults	initial cost: € 2,470.59 annual upgrade: € 500.00	annual maintenance: € 282.35	0.65	0	1000 €

Table 5: Economic evaluation of risk reduction security measures in relation to unauthorized alterations of website contents

		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	1364.24	500.00	282.35
2	0.05	384.47	0.00	0.00	1364.24	500.00	282.35
3	0.05	384.47	0.00	0.00	1364.24	500.00	282.35
4	0.05	384.47	0.00	0.00	1364.24	500.00	282.35

Table 6: Calculation of ROI, NPV and IRR risk reduction security measures in relation to unauthorized alterations of website contents

Measure	ROI	NPV	IRR
A	26%	140.16 €	10%
B	-3%	-407.26 €	-2%

incident. Investing in measures related to information security is therefore inevitable for all organizations that are either included in the process of electronic commerce.

Persons who are responsible for investment are wondering about the best solution for investment and in particular about the amount of the investment. . Before investing in a particular measure it is good to know whether the investment is financially justified. Investment in information security technology and measures is no exception. The economic approach to managing security risk assessment and selecting optimal measure in information security is typically a large project. It implies a thorough analysis and evaluation of information assets, analysis of threats attacking information assets, analysis the consequences of information technology failure, analysis of the probability for a success attack and assess the costs and benefits resulting from investment in information security.

In the paper a comprehensive model for managing the information security risks is described. The model allows evaluation of investments in security and protection of business information systems. The model is based on quantitative analysis of security risks and allows evaluation of different investment options. The model is designed as a standard procedure, which leads organization from the initial input data selection to the final recommendations for the selection of an optimal measure that reduces a certain security risk. The biggest advantage of the model is that it allows direct comparison and quantitative evaluation of the various security measures: technological security solutions, the introduction of organizational procedures, training or transfer risk to an external company. The output data of the model is the profitability of each security measure as measured by ROI, NPV and IRR and comparison of individual measures with each other.

9 Literature

Acquisti, A., Friedman, A. & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In: *Workshop on the Economics of Information Security,* UK: Cambridge, Retrieved October 12, 2012 from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Anderson, R. & Schneier, B. (2005). Guest Editor's Introduction: Economics of Information Security. *IEEE Security and Privacy*, 3(1), 12-13, http://dx.doi.org/10.1109/MSP.2005.14

Anderson, R. (2001). Why information security is hard-an economic perspective, Computer Security Applications. In: *ACSAC 2001, Proceedings of the 17th Annual Conference*, pp. 358–365, http://dx.doi.org/10.1109/ACSAC.2001.991552

Bojanc, R. & Jerman-Blažič, B. (2007). Towards a standard approach for quantifying an ICT security investment. *Computer Standards*

& Interfaces, 30(4), 216-222, http://dx.doi.org/10.1016/j.csi.2007.10.013

Bojanc, R. & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), 413-422, http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.002

Bojanc, R., Jerman-Blažič, B. & Tekavčič, M. (2012). Managing the Investment in Information Security Technology by use of Quantitative Modeling Approach, *Information Processing & Management*, 48(6), 1031-1052, http://dx.doi.org/10.1016/j.ipm.2012.01.001

Cavusoglu, H., (2004). Economics of IT Security Management. In: Camp, L. and Lewis, S. (Eds), *Economics of Information Security*, Vol. 12, pp. 71-83. Springer US, http://dx.doi.org/10.1007/1-4020-8090-5_6

Computer Security Institute (CSI). (2011). 2010/2011 Computer Crime and Security Survey. The 15th Annual Computer Crime and Security Survey. Retrieved January 17th, 2012, from http://www.gocsi.com/survey

Farahmand, F., Navathe, S., Enslow, P. & Sharp, G. (2003). Managing vulnerabilities of information systems to security incidents. In: *ICEC ,03 Proceedings of the 5th international conference on Electronic commerce*, pp. 348–354. ACM: New York, USA, http://dx.doi.org/ http://dx.doi.org/10.1145/948005.948050

Gordon, A. L. & Loeb, P. M. (2001). Using information security as a response to competitor analysis systems. *ACM*, 44(9), 70–75, http://dx.doi.org/10.1145/383694.383709

Gordon, A. L. & Loeb, P. M. (2002). The Economics of Information Security Investment. *ACM,* 5(4), 438-457, http://dx.doi.org/10.1007/1-4020-8090-5_9

Gordon, A. L., & Richardson, R. (April 13, 2004). The New Economics of Information Security. *Information Week*, 53-56. Retrieved February 11th, 2007, from http://www.banktech.com/aml/showArticle.jhtml?articleID=18901266

Hoo, S. (2000). *How Much Is Enough? A Risk-Management Approach To Computer Security*. Retrieved February 28th, 2010, from www.cl.cam.ac.uk/~rja14/econws/06.doc

International Organization for Standardization. (2005). *Information technology – Security techniques – Information security management systems – Requirements.* ISO/IEC 27001:2005. Geneva.

International Organization for Standardization. (2009). *Information technology – Security techniques – Information security management systems – Overview and vocabulary.* ISO/IEC 27000:2005. Geneva.

Matsuura, K. (2009). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. In: *Managing Information Risk and the Economics of Security*, pp. 99-119. Springer US, http://dx.doi.org/10.1007/978-0-387-09762-6_5

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

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

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

Ryan, J., & Ryan, D. (2006). Expected benefits of information security investments. *Computers & Security*, 25(8), 579–588, http://dx.doi.org/10.1016/j.cose.2006.08.001

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

Schneier, B. (2004). *Secrets & Lies, Digital Security in a Networked World*. New York: Wiley Publishing.

Tanaka, H., Liu, W. & Matsuura, K. (2006). An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan. In: *Workshop on the Economics of Information Security*, UK: Cambridge. Retrieved October 12, 2012, from http://weis2006.econinfosec.org/docs/9.pdf

Tanaka, H., 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(1), 37-59, http://dx.doi.org/10.1016/j.jaccpubpol.2004.12.003

Willemson, J. (2006). On the Gordon and Loeb Model for Information Security Investment. In: *Workshop on the Economics of Information Security*, UK: Cambridge, Retrieved October 12, 2012, from http://weis2006.econinfosec.org/prog.html

---

Rok Bojanc obtained his Ph.D. in the field of Management Information Science from the University of Ljubljana. He works as an IT Manager at ZZI, a software solution firm 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 for more than ten years. He is the author and co-author of several scientific articles published in recognized international journals. He has written many handbooks, technical articles and training courses for subjects including IT, networks, security, and information systems. He frequently lectures at conferences and seminars.

Borka Jerman-Blažič is a full professor at University of Ljubljana, Department of Economics and is heading the Laboratory for Open Systems and Networks at Jožef Stefan Institute. The Laboratory under her leadership is involved more than twenty years in European Union Framework Program projects in the area of ICT and related field (www.e5.ijs.si). At the University of Ljubljana, Faculty of Economics as a Full Professor she is teaching courses in electronic communications and information security. She is teaching as well postgraduate courses in Telecommunication Services and Technologies, Legal aspects and standards in ICT and E-commerce. She is teaching ICT Security in e-commerce at the Postgraduate School of Criminal Justice, University of Maribor and at the postgraduate international school Jožef Stefan. She has spent her postdoctoral at Iowa State University, Ames, USA and has worked as a project development officer for TERENA – The European Association of Academic and Research Networks. She is also acting as research adviser to the Security Unite of Stockholm University, Department for Computer and Systems Sciences.

Prof. Jerman-Blažič was leading research teams in many EU funded projects, most of them from the ICT Framework Program 4th , 5th , 6th , and 7th and was acting as evaluator and auditor. The last project she was working from FP7 was EIFFEL-Evolving Future Internet For European leadership. She is member of the editorial board of two international journals: International Journal on advances in internet technology, and International Journal of technology enhanced learning.

Prof. Jerman-Blažič is a member of the Scientific Council of the European Privacy Association and member of the FP7 SECURITY programming committee in DG Enterprise. She was appointed member to UNECE/CEFAT UN (Economic

Commission for Europe) group for Internet enterprise development, Ex-Chair of the Internet Society of Europe (www.isoc-ecc.org) in the first mandate (2004-2007), Distinguished Member of Slovene Society for Informatics, member of New York Academy of science, member of the editorial board of the international journal of Technology Enhanced e-Learning and International journal on advances in Internet technology. She is also member of the Grand Jury of United Nations for the e-content awards of WSIS and member of the State Council for electronic Communications. She is also Chair of Slovenian Standardisation Committee on ICT as well as chair of the Slovenian chapter of Internet Society and is member of the European ICT Standardisation Board (ICTB). Prof. Jerman-Blažič has published more than 300 articles in international journals, conferences, books and was an invited speaker in many international conferences and workshops. She is holding the ACM and IEEE Thai Section Plaque for significant achievement in the Internet technology.