Management,
Knowledge and Learning
International Conference 2012

QUANTITATIVE MODEL FOR INFORMATION SECURITY RISK MANAGEMENT

Rok Bojanc
ZZI d.o.o.
rok.bojanc@zzi.si

Abstract:
The paper presents a mathematical model to improve our knowledge of information security and risk management in contemporaneous businesses and other organizations. In the world of permanent cyber-attacks to information systems the knowledge about risk management is becoming a crucial task for minimization of the potential risks that can endeavour their operation. Therefore, it requires good knowledge of information security. The prevention of the heavy losses that may happen due to cyber-attacks and other failures in an organization is usually associated with knowledge about appropriate investment in different security measures. With the rise of the potential risks from different cyber-attacks the investment in security services and data protection is growing and is becoming a serious economic issue to many organizations and enterprises. 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 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.

Keywords: information technology management, modelling security technology, risk management.

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.

Trends like globalization, higher productivity and reducing the costs makes the business organizations increasingly dependent from their information systems and the Internet services. Potential attack on the information systems and eventual crash may cause heavy losses on data, services and business operation. Security risks are present in the organization's information system due to technical failures, system vulnerabilities, human failures, fraud or external events. This is the main reason why organizations are investing in information security systems, which are designed to protect the confidentiality, integrity, and availability of information assets. Due to the rising awareness regarding the potential risks of attacks and breaches the investments in information security are increasing and are take different approaches depending of the area of applications. Although security technologies have made a great progress in the last ten years, security level of computers and networks has never been considerably improved.

In the past, the knowledge in information security cannot devote excessive attention. Determination of threat was countered by seeking a technical solution to prevent this threat. 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 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. 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.

Obtained knowledge on information security opens up many questions on which the presented model can provide the answers; How to provide security for the IT-based operations? Which security level is adequate? How much money should be invested in security? Organizations 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. 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. 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. 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.

This paper tries to propose a standard approach obtaining knowledge about information security and risk management. Today's world urgently needs a better knowledge on information security. It is necessary to know the threats that have become a global where the attacker can be anywhere. There are a lot of security measures and a good knowledge is needed to select the appropriate action. There is an urgent need for cooperation and integration between IT, organization and human resources, because only together organization can gain sufficient knowledge of effective information security. This is also related to the continuing education of employees in information security.

2. COMBINING KNOWLEDGE OF INFORMATION SECURITY AND ECONOMICS

Information security was traditionally considered as a technical discipline, whose purpose was to provide the maximum level of security. In the last decade, a major economic component was considered in the related research as investments in information security are rapidly increasing. Information security economics, a relatively new field of study, uses economic theory and models to analyse incentives between the involved stakeholders. Information security should be viewed not just as a cost, but as a value creator that supports and enables e-business operations. Knowledge about investments in information security requires quantification of costs and benefits of the investments in a comparable way. 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. The optimal level of information security investments is treated on the basis of the expected cost/benefit investment trade-offs.

One of the key issues of information security is to obtain knowledge of how much the organization should invest in information security operations. A decision is not easy. The problem combines the uncertainty about the threats, vulnerabilities, consequences of a successful attack and efficiency measures. It is important that the organization is aware that the security measures only reduce the risk to an acceptable level and that 100 % security is not and should not be an objective. Security investments cannot be measured solely by technical indicator, or over the amount of invested money, but through a systematic analysis of the costs of security measure and benefits for its implementation (Schechter, 2002).

Cost-benefit analysis compares the costs of certain activities to the benefit that activity produce (Gordon & Loeb, 2002). Let us assume that we can estimate the expected total benefits and the expected total cost for different levels of information security activities. As long as the additional benefits of information security activities outweigh the costs, the implementation of activities is rational. The organization's goal should be the implementation of security measures to the point where the benefits minus the costs have a maximum value. The implementation of information security activities over this point means that the marginal costs of additional security are greater than marginal benefits of additional security. In other words, the net benefits (i.e. benefits minus costs) of implementation of information security

over maximum point are negative. For the organization does not make sense a spending more for a security measure than the potential loss in case of a security incident. However, an organization can continue to invest in security activities until the marginal benefits are equal to the marginal cost (Gordon & Loeb, 2005).

Costs for security measures are calculated quite easily, this is the money that the organization spent on particular investment, which aims to reduce security risks. Unlike the costs which are 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) per se do not bring financial benefits that can be measured. The most common benefits of investment in information security are the reduction of occurrence of the incidents and consequently the losses caused by the incidents

In general, the benefits of investment in information security are commonly taken as the cost savings from reducing the likelihood or consequences of security incidents (Gordon & Loeb, 2005). These benefits are often very difficult to be predicted very accurately. The biggest problem lays in the assessment of the cost savings related to potential security incidents that have not yet occurred. The more successful information security is, the harder it is to notice and calculate the benefits.

In the next chapter will present a mathematical model for calculating costs and benefits of implementation for different security countermeasures.

3. QUANTITATIVE RISK MANAGEMENT

3.1. Risk assessment

The goal of security risk assessment is to identify and measure the risks in order to inform the decision making process. Risk analysis needs the data about information assets in organization, threats to which assets are exposed, system vulnerabilities that threats may exploit and implemented security controls (Bojanc, Jerman-Blažič & Tekavčič, 2012).

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

Information assets may have vulnerabilities. Vulnerability is a weakness in security procedures, technical controls, physical controls, or other controls of an asset that a threat may exploit. Most security incidents are caused by vulnerabilities presented by flaws in software. Vulnerabilities are typically known as a technical issue, however there are vulnerabilities caused by human factor. This type of vulnerabilities are caused by users sharing their passwords or using weak passwords, by not understanding or ignoring security policies, opening non trusted e-mail, visiting web sites, or downloading software that contains malicious code.

An organization's information assets are exposed to threats. A threat is any potential event with an undesirable impact. The common threats to organizational assets are distributed between natural disasters and human acts, where the threats caused by humans can be malicious or non-malicious. Some typical examples of malicious human threats are theft, loss or destruction of an organizational asset, fraud, unauthorized access to the network services, infection with malicious code, disclosure of someone's personal data and identity theft.

Some of the attacks can be successful, resulting in a security incident, while others are not successful. Probability of a security incident occurrence is the number of times that an organization reasonably expects a particular threat to occur during a single year. Probability of a security incident ρ can be calculated as the product of the threat probability T and asset vulnerability v.

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

Threat probability T is defined as a probability of an attack on information assets. Threat probability equals the number of attacks per unit of time. System vulnerability v is defined as a probability of a threat that is successfully realized in a form of an incident on an information asset. Calculating estimations for the probability of a security incident occurrence is very difficult. There is very little actuarial data available, as only a few companies successfully track security incidents and report on them.

In case of a security incident, the organization suffers financial loss L, which 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. Indirect loss represent damage to the reputation of the organization, the interruption of business processes, legal liabilities, 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. The quantitative evaluation of loss can be supported through the allocation of losses to individual factors. The first part which depends on t_r, the second part which depends on t_d and third part which is not time dependent:

$$L = L_1 \cdot t_r + L_2 \cdot t_d + L_3 \tag{2}$$

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:

$$R = \rho \cdot L = T \cdot v \cdot \left[L_1 \cdot t_r + L_2 \cdot t_d + L_3 \right] \tag{3}$$

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).

3.2. Risk treatment

There are multiple strategies available to treat each security risk (NIST, 2002). 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, access control, port blocking etc.). 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 is becoming in the last period an increasingly important strategy for applying 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 asset e.g. full open connectivity to Internet.
- Acceptance of security risk as a part of business operations. Risk retention is a reasonable strategy for risks where the cost of investment or insuring against the risk would be greater over time than the total losses sustained.

Combination of these 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.

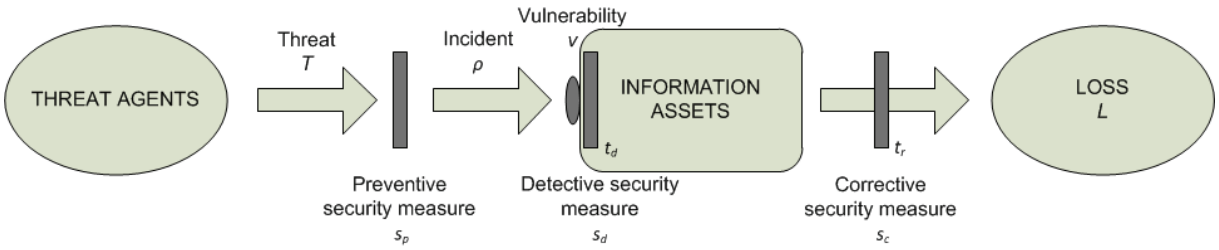
3.3. Security measure selection

An organization protects itself from potential security attacks by implementing security measures that can be classified into three categories according to their impact on the 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).

Picture 1 shows the points where different types of security measures are integrated into the model.

Picture 1: Security model



Source: Bojanc, Jerman-Blažič & Tekavčič, 2012.

Detective security measures enable a detailed analysis of the security events, detect incidents, and warn against them. Therefore detection security measures are crucial to obtain better knowledge about threats. The use of detective protection enables loss reduction and a more realistic assessment of attack probability T, and incident probability ρ. When organizations

are not using detective controls, the probability values are merely an estimate and they can differ much from realistic values. Wrong assumptions can also lead to non-optimal selection of security measures.

Each security measure s is defined by two quantitative parameters productivity of measure α and cost of measure C. Security measure productivity α presents the impact of a security measure on the risk reduction. Cost of measure C is a monetary investment in security measure and takes in account all expenses related to the implementation of the selected security measure. It includes purchase, implementation, testing, training and maintenance cost.

Security measures s reduce security risk R. The security incident probability ρ can be reduced by introducing a preventive security measure s_p. Various incident probability ρ functions are available (Gordon & Loeb, 2002). In the presented model we used:

$$\rho(T, v, C_p) = T \cdot v^{\alpha_p C_p + 1} \tag{4}$$

The loss L resulting from security incidents can be reduced with an investment C_c into a corrective security measure s_c and with an investment C_d into a detective security measure s_d. Corrective security measures reduce the time to repair, consequently reducing the loss caused by the incident while detective security measures reduce the time to detect security incident. One of the possible security measures according to the risk treatment options 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. Losses incurred due to a security incident can be written down as:

$$L = L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_c C_c} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \tag{5}$$

Considering equation (3) the probability function intrusion ρ (4) and loss L (5), the quantitative equation for security risk is calculated as:

$$R = T \cdot v^{\alpha_p C_p + 1} \left[L_1 \cdot t_r^{\,0} \cdot e^{-\alpha_c C_c} + L_2 \cdot t_d^{\,0} \cdot e^{-\alpha_d C_d} + L_3 - I \right] \tag{6}$$

The benefits B of investment in security measure are equal to the risk reduction due to the implementation of a security measure:

$$B = R_0 - R \tag{7}$$

Where R_0 is the security risk prior to the implementation of a security measure and R is the security risk after the implementation of a security measure.

3.4. Return on security investment

The economic impact of a certain measure can be analysed with the cost-benefit approach. For this purpose the Return on Investment (ROI), Net Present Value (NPV), and Internal Rate of Return (IRR) are used[1] (Bojanc & Jerman-Blažič, 2008).

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:

[1] In the CSI Survey [2011] ROI, NPV and IRR are the most often used security metrics in practice.

$$ROI = \frac{B - C}{C} \tag{8}$$

The result is investment profitability expressed in percentages; positive ROI value means that an investment is economically justified.

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 (NVP) 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):

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} \tag{9}$$

In this case, B_t denotes present value of the net benefits of period t, C_t denotes all costs, i denotes the discount rate and n denotes the time period. NPV is measured in monetary units, while an investment is economically justified when NPV>0.

Internal Rate of Return (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.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^t} = 0 \tag{10}$$

When comparing the two parameters for the cost and benefit analysis it is necessary to consider ROI, NPV and IRR, because each of them can point to a different optimal solution (Bojanc & Jerman-Blažič, 2008). 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 difficult to achieve since it frequently happens 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. For this reason, a comparative risk management analysis is proposed.

4. CONCLUSION

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 model makes use of the quantitative analysis of different security measures that counteract individual risks by identifying information processes within an organization and potential threats. The model comprises the target security levels for all identified core business processes and the probability of a security accident together with the possible loss that may be suffered by the organization. The selection of security technology is based on the efficiency of the security measures selected. Economic metrics are applied for efficiency assessment and comparative analysis of different protection technologies. 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 core 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.

The presented methodology and mathematical model for the optimal selection of investments into security technology for the protection of the corporate information systems, is based on a quantitative security risk analysis. The model allows a deep analysis and computations for quantitative assessments of different investment options which translate into recommendations facilitating the decision-making process and the selection of the best security investment. The quantitative risk assessment of the business processes, as provided in the model, enables a detailed overview of threats expressed in financial values that are of great interest to managers who are responsible for the final investment decisions. With this model, the necessary investments are approved in a much faster fashion, since the quantitative assessment results provide the basis for a fast and simple comparative analysis of investment efficiency, and consequently make the decision-making more qualitative and efficient. Each of indexes presented in this paper, ROI, NPV and IRR have their benefits but each of them used individually does not present appropriate solution. Therefore, the best way to assess the required investment is the use of combination of these methods.

REFERENCE LIST

1. Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management, *International Journal of Information Management, 28*(5), 413–422.
2. Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the Investment in Information Security Technology by use of Quantitative Modeling Approach, *Information Processing & Management* (pp. 22), Retrieved from http://dx.doi.org/10.1016/j.ipm.2012.01.001
3. Gordon, A. L., & Loeb, P. M. (2002). The Economics of Information Security Investment. *ACM 5*(4), 438–457.
4. Gordon, A. L., & Loeb, P. M. (2005). Managing Cybersecurity Resources: A Cost-Benefit Analysis, New York: McGraw Hill.
5. Hoo, S. (2000). How Much Is Enough? A Risk-Management Approach To Computer Security, *Palo Alto*, CA:Stanford University.
6. NIST. (2002). NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html
7. Schechter, S. (2002). Quantitatively differentiating system security. *Workshop on the Economics of Information Security (WEIS 2002).* Retrieved from http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/