Towards a standard approach for quantifying an ICT security investment

Rok Bojanc, Borka Jerman-Blazič *

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

Available online 22 October 2007

Abstract

The rise of the potential risks from different attacks on ICT systems means the investment in security technology is growing and is becoming a serious economic issue for many organizations. The assessment of the appropriate investment that is economically affordable and provides enough protection for the enterprise information system is an issue that is analysed here. The paper discusses the identification of the assets, the threats, the vulnerabilities of the ICT systems and provides an approach for the quantification of the necessary investment. The paper concludes with a recommendation for a standard approach to security-information investment assessment.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Security technology investment; Cyber crime prevention; Information security

1. Introduction

The continued growth in the use of information technologies for business purposes makes business organizations increasingly dependent on their information systems. Any successful attack on an information system and its eventual crash could result in a serious loss of data, services and business operations. This is the main reason why modern organizations are investing in information-security measures and data-protection systems. Almost a decade ago a number of researchers began to realize that security and privacy are not simply a technical problem; there is a major economic component as investments in information security are increasing very rapidly. Security risks are present in an organization’s information system because the system has vulnerabilities and because of human–computer interactions. Losses from security breaches can be caused by a poor organisation of security measures, human failures or fraud, technical failures or external events, and accordingly they are classified as financial, technical, ecological, social, psychological or other. In the context of business operations the meaning and the importance of security failures are better understood through economic losses than with a technical analysis. This is the reason why the focus on the prevention of possible failures and cyber crime is shifting from what is technically possible to what is economically optimal [2].

When looking at cyber crime prevention and the provision of secure ICT from the economic point of view, some common questions arise: How does an organization become secure in terms of its IT-based operation? Which security level is appropriate? How much money should be invested in security? The answers to these questions are not straightforward; however, they need to be answered before any substantial investment is made in a security solution.

In order to determine how much an organization should spend on IT security and data protection it is important to know the value of the assets to be protected. In this way the most cost-effective solution can be determined. This is usually done by risk management, which provides the organization with information about the consequences if appropriate protection and security solutions are not provided and about the potential losses in the case of a security incident and the impact it may have on the company’s overall productivity. This paper proposes a standard procedure for the assessment of an ICT security investment. In the proposed approach the identification of the assets, the threats, and the vulnerabilities of the ICT systems are first identified through a risk-management analysis followed by the introduction of metrics for the quantification of the investment. The paper ends with a discussion of the applicability of the approach.
From overall reports it is obvious that the number of privacy and security incidents is growing. Privacy incidents are always related to the misuse or the revealing of someone’s personal data of any kind, and these are considered as severe as any other type of security incident. Generally speaking, individual users of internet services are already aware of privacy risks and often pay for goods or services that will enhance their privacy [14]. Organizations in some parts of the world (for example, the EU) are obliged by law to introduce the appropriate protection of personal data within their customer databases and whenever these data are being processed, used or stored.

Identity theft is a combined security and privacy risk; it is also known as impersonation fraud. Identity theft is the illegal use of an individual’s personal identifying information (such as name, address, date of birth, credit-card number, etc.) to impersonate that person and commit financial fraud. The actual cost of such an attack to the victim can be quite severe; there is the loss of credit rating and the resources spent on fixing financial records, which can often take years [1]. Studies completed by Gartner Research indicate that from July 2005 to July 2006 approximately fifteen million people were the victims of identity theft [8].

Security experts agree that the number of security breaches is vastly under-reported. Government and industry sources estimate that only 20% of computer security violations are actually reported and many serious and costly security failures are never revealed. These enterprises deal with the problems internally, fearing a disaster in public relations, a devastating loss of consumer confidence, or worse, revealing their vulnerability to other hackers.

2.2. Identifying the vulnerabilities and the potential loss

Vulnerability is the weakness of an asset that a threat may exploit. Most security incidents are caused by vulnerabilities represented by flaws in the software. Some researchers define such vulnerabilities as tradable externalities and the specific goods that are considered to be the medium of exchange in the various security markets [3]. Some organizations in a vulnerability market are acting as “infomediaries”, which offer a monetary reward to the identifier of every vulnerability reported to it. The infomediary then shares this information with their subscribers. An infomediary may deliver a patch to fix the vulnerability or provide filters to protect against attacks that exploit the vulnerability. In this way subscribers can protect themselves against attacks that exploit those specific vulnerabilities.

The best-known solution for software vulnerabilities is the application of patches, which are generally released by software vendors to fix the vulnerabilities in their software products. The time window between the identification of vulnerabilities and the creation of exploits has shrunk dramatically over the years. However, it is well known that many systems are often left unpatched for months (or even years) even though the updates are widely available. The consequences of not updating systems promptly with the necessary patches can be severe damage, such as that caused by the NIMDA, SQL Slammer, Code Red and Blaster worms that affected hundreds of thousands computers and caused enormous damage.
It is widely recognized that organizations have become so dependent on information systems that a disruption to any part of the system may cause outcomes ranging from inconvenience to catastrophe. In recent years an increase in the number of security breaches that led to major losses for the affected organizations was recorded and reported. These losses are due to a security breach related to confidentiality, the integrity of data, or due to a denial of services. Among them the impact of confidentiality-related security breaches is associated with most significant losses in terms of the organization’s assets value [4].

The data concerning the true cost of a security incident is very difficult to find. One of the reasons for this is that most organizations do not systematically track and document security incidents. Currently, the most up-to-date actual data comes from the efforts and results presented in the annual CSI/FBI survey report [6]. The identified impact of an information security breach is counted in terms of immediate losses and indirect losses. Immediate losses are losses of revenue, losses of productivity and increased costs. In many situations the actual immediate loss remains a small part of the overall loss due to security incidents. Usually, indirect losses appear to be more serious as they have a much longer negative impact on the customer base, the supplier partners, financial market, banks and business alliance relationships, and these costs are sometimes even higher than the immediate costs caused by the security breach. Indirect losses represent damage to the reputation of the organization, the interruption of business processes, legal liabilities, loss of intellectual property, and damage to customer confidence.

3. Quantifying the risk assessment

A risk assessment helps organizations to assess their risk and to identify and prioritize security measures within the organization. It helps in taking a decision regarding the necessary investment in security controls and systems in areas that maximize the business benefit. There are many different methodologies for assessing risks, but most are based on one of two approaches or a combination of the two: a quantitative risk analysis or a qualitative risk analysis.

A quantitative risk analysis attempts to assign numeric values to the likelihood and the impact of the risk and to the costs and benefits related to the introduction of security controls and systems. The purpose of the IT security infrastructure is to mitigate the risk up to a point where the marginal cost of implementing controls is equal to the value of the additional savings from security incidents. The problem with a quantitative risk analysis is in the non-existence of a standard and proved method that will effectively calculate the values of the assets and the cost of the controls and systems that need to be applied. In contrast to the quantitative approach, a qualitative risk analysis attempts to calculate relative values instead of assigning exact financial values to assets, expected losses, and the cost of controls and systems. A qualitative risk analysis is usually conducted through a combination of questionnaires and collaborative workshops. The advantage of a qualitative approach is that the process itself demands fewer staff and an accurate calculation of the asset value and the cost of the control are not required. The drawback of the qualitative approach is in the resulting figures, which are usually vague as they are derived as relative values of the assets.

The exposure to a risk can be measured with different quantitative techniques. A very simple analytical method, risk exposure quantification, uses metrics known as Single Loss Exposure (SLE), Annual Rate of Occurrence (ARO) and Annual Loss Expectancy (ALE).

The Single Loss Exposure (SLE) is the total amount of revenue that is lost from a single occurrence of the risk. It is a monetary amount that is assigned to a single event that represents the organization’s potential loss if a specific threat exploits a vulnerability. The SLE is calculated by multiplying the asset value (AV) by the exposure factor (EF).

\[
SLE = AV \times EF
\]

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

The Annual Rate of Occurrence (ARO) is the number of times that an organization reasonably expects a particular risk to occur during a single year. Calculating estimations for the SLE or ARO is very difficult. There is very little actuarial data available, as only a few companies successfully track security incidents and report on them.

Security-risk exposure is calculated by multiplying the annual rate of occurrence by the single loss expectancy. The product is called the Annual Loss Expectancy (ALE), which represents the total amount of money the organization could lose in one year if nothing is done to mitigate the risk.

\[
ALE = SLE \times ARO
\]

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

4. Quantifying the assessment of the information-security investment

The natural reaction of a business to growing security risks and potential security breaches is recorded by the company’s increased investment in security technologies. The purpose of the investment is to lower the probability of security breaches and to minimize the security risks. However, this probability is not very high. According to a DTI 2006 survey the average is around 4–5% of the organization’s IT budget being spent on security solutions [7].

It is clear that the optimal level of information-security investment depends on the cost/benefit tradeoffs, and this is the
reason why the costs of the information-security investment in the models are compared to the expected benefits [11]. Some researchers are suggesting a cost-effective analysis, rather than a cost-benefit analysis, as the costs and benefits are not commensurate [9]. An alternative method that tries to analyze the optimal information-security investment is based on what is known as game theory. Game theory uses the interaction between a potential hacker and the organization and tries to explain situations of intrusions where the hacker has a motive to attack and cause damage to a particular organization [5].

Most of the currently used metrics for quantifying the costs and benefits of computer-security investments are based on calculated indicators such as the Return on Investment (ROI), the Net Present Value (NPV), the Internal Rate of Return (IRR) or combinations of all of these.

### 4.1. Return on Investment (ROI)

Return on Investment (ROI) is a popular metric for the comparison of technology investments in the area of business. The fundamental question that ROI is designed to answer is: which of these options gives me the most value for my money? For example, a company might use ROI when deciding whether to invest in the internal development of a new technology/solution or to purchase a commercial product/solution.

ROI simply defines how much the organization gets from the amount of money spent. The indicator is expressed as a percentage of the returned investment over a specific amount of time. ROI equals the present value of the accumulated net benefits over a certain time period, divided by the initial costs of the investment.

\[
ROI = \frac{\text{Benefits} - \text{Cost of Investment}}{\text{Cost of Investment}}
\]

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

The cost of information-security investments should be considered as a compound of the system-configuration specific costs and the operating costs. System-configuration specific costs are typically a one-time expense for the purchase (or development), testing and implementation of a defense solution that protects information assets from possible threats. The operating costs are represented by the annual maintenance (upgrades and patching of the defense solution), the training of users and network administrators, and the monitoring of the solution. The cost of the security investment could be initially low, but later it can increase due to the needs for higher levels of security infrastructure in the organization.

On the other hand it is very difficult to define, assess or measure the benefits. Firewalls, IDS, antivirus software and other security solutions simply do not generate revenue that can be measured. Therefore, the gain produced by this investment becomes a subjective number. One way that makes it possible to assess the benefits of information-security investments is to estimate the avoided damage, expressed in terms of the probability of an event occurring. The benefits can be then be represented as the difference between the ALE without any security investment and the ALE with a security investment.

\[
\text{benefits} = \frac{\text{ALE}_{\text{without investment}} - \text{ALE}_{\text{with investment}}}{\text{Cost of Investment}}
\]

In the Gordon–Loeb model, where the ALE (with investment) is represented as a function of the investment and the vulnerability, the optimal investments in information security range from 0% to 36.8% of the potential loss due to a security breach [10]. This model has since also been successfully used in some empirical analyses [13]. It can be claimed that according to this model, benefits will initially increase rapidly and later the benefit growth is stabilized due to the reduction of the probability of security breaches. A simple equation for calculating the Return on Security Investment (ROSI) is as follows:

\[
\text{ROSI} = \frac{\text{ALE}_{\text{without investment}} - \text{ALE}_{\text{with investment}} - \text{Cost of Investment}}{\text{Cost of Investment}}
\]

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

\[
\left(\frac{\text{€8750} - \text{€3400} - \text{€1600} - \text{€450}}{\text{€1600 + €450}}\right) = 160\%
\]

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

### 4.2. Net Present Value (NPV)

In the case of long-term investments the time attribute represents a problem when calculating the ROI, and managers are mainly using the index known as the Net Present Value (NVP) along with ROI to justify expenditure. The methodology behind the NPV is in the assessment of the tax cash flows generated by a particular solution and in the assessment of the cash-flows value in the current cash flow of the enterprise. The cash-flows index consists of the value of the initial investment, the cost of installation, the cost of configuration, the cost of maintenance and the cost of updates.

The NPV is useful in cases when alternatives are being evaluated. For example, an organization chooses between two security solutions, where one costs €15,000 in advance, and the other costs €5000 a year for three years. Both solutions cost €15,000, but the second solution is better because the organization can invest the remaining money in other places for a defined time. Therefore, the real cost of the second solution is less than €15,000.
The NVP gives the value of the cash return that is expected and is calculated by summing the present net value of the benefits for each year over the expected lifetime periods and by subtracting the initial costs of the project. Suppose $B_i$ is the present value of the net benefits for the period $i$, $C_i$ is all the costs and $i$ is the internal rate of discount. The NPV of the investment is calculated as follows:

$$\text{NPV} = \sum_{i=0}^{n} \frac{B_i - C_i}{(1 + i)^t}$$

(6)

A positive NPV means that the project generates a profit, while a negative NPV means that the project generates a loss. Therefore, a project is profitable if the NPV exceeds zero. An important characteristic of the NPV is that it provides us with information about the cash value of the expected return and therefore indicates the magnitude of the project; the drawback is in the lack of information about the time over which the expected return occurs.

4.3. Internal Rate of Return (IRR)

The Internal Rate of Return (IRR) is often used to analyze large, long-term investments. The IRR is calculated by using a cash flow like the NPV. Unlike the NPV calculation, the IRR will show at what rate it will break even. The IRR equals the percentage rate at which the discount rate should be applied in order that the benefits obtain a zero NPV.

$$\sum_{i=0}^{n} \frac{B_i - C_i}{(1 + \text{IRR})^t} = 0$$

(7)

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

Each of these financial measures has its own strengths and weaknesses. The ROI has a difficulty in defining the magnitude of the investment. The NPV and IRR both have difficulty in figuring the ALE. In most cases, the NPV and IRR are better indicators than a simple ROI calculation [12]. To get a clear and complete picture of a planned investment, the standard approach should be based on all of these measures.

According to a 2006 CSI/FBI Survey, 42% of organizations use Return on Investment (ROI) as a metric, 19% of them use Net Present Value (NPV) and 21% use the Internal Rate of Return (IRR). Although ROI has a number of limitations, when compared with NPV and IRR, ROI is still by far the most popular metric in use [6].

4.4. A practical illustration

To illustrate their merits a comparison of these metrics is provided in the next example. An organization with 500 computers intends to purchase new antivirus software (AV) and it is choosing between alternatives. Some antivirus software successfully detects more viruses, while others are less efficient. An antivirus software “AV-A” detects 96% of all viruses. Its purchase price is €60 per licence, while the annual renewal price is €25 per licence. The antivirus software “AV-B” detects only 64% of all viruses, but it costs only €50 per licence with lifetime support, which means the renewal price is zero. In addition, the organization estimates that yearly maintenance costs (updates, monitoring, and upgrades) will be €5000 for AV-A and €4000 for AV-B. The benefits with this purchase can be estimated with the ALE. We propose the following modified Eq. (4) for this example:

$$\text{Benefits} = \text{ALE}_{\text{without AV}} - \text{ALE}_{\text{with AV}}$$

$$= \text{ALE}_{\text{without AV}} \times \text{AV software effectiveness}$$

The ALE can be calculated with the following Eqs. (1) and (2):

$$\text{ALE} = \text{SLE} \times \text{ARO} = \text{AV} \times \text{EF} \times \text{ARO}$$

In the case of simultaneous virus infection on all computers in an organization and a consequent inability to do business on one, the asset value (AV) is €60,000. In reality, when the infection occurs, only one third of computers get infected and it takes on average 2 h to cleanup a computer. Therefore, the EF is $0.33 \times 0.25 = 8.25\%$. The ARO is estimated on the basis of 15 incidents per year.

$$\text{ALE} = €60,000 \times 0.0825 \times 15 = €74,250$$

Benefits$_{(\text{AV-A})} = €74,250 \times 96\% = €71,280$

Benefits$_{(\text{AV-B})} = €74,250 \times 64\% = €47,520$

An organization will use the selected antivirus solution over the next five years. In Table 1 the benefits are represented together with the costs for both solutions. So, let us do the ROI calculation first. From Eq. (3) we get the results:

$$\text{ROI}(\text{AV-A}) = 203\%$$

$$\text{ROI}(\text{AV-B}) = 428\%$$

<table>
<thead>
<tr>
<th>Year</th>
<th>AV-A Benefits (€)</th>
<th>Purchase and upgrade costs (€)</th>
<th>Maintenance costs (€)</th>
<th>AV-B Benefits (€)</th>
<th>Purchase and upgrade costs (€)</th>
<th>Maintenance costs (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30,000</td>
<td></td>
<td></td>
<td>25,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>71,280</td>
<td>12,500</td>
<td>5000</td>
<td>47,520</td>
<td>12,500</td>
<td>4000</td>
</tr>
<tr>
<td>2</td>
<td>71,280</td>
<td>12,500</td>
<td>5000</td>
<td>47,520</td>
<td>12,500</td>
<td>4000</td>
</tr>
<tr>
<td>3</td>
<td>71,280</td>
<td>12,500</td>
<td>5000</td>
<td>47,520</td>
<td>12,500</td>
<td>4000</td>
</tr>
<tr>
<td>4</td>
<td>71,280</td>
<td>12,500</td>
<td>5000</td>
<td>47,520</td>
<td>12,500</td>
<td>4000</td>
</tr>
<tr>
<td>5</td>
<td>71,280</td>
<td>12,500</td>
<td>5000</td>
<td>47,520</td>
<td>12,500</td>
<td>4000</td>
</tr>
</tbody>
</table>
So far it looks like AV-B is the favourite solution, but as was shown above, the ROI provides information on the percentage of the value of return only and not the actual magnitude. In this case Eq. (6) is used for calculating the NPV, and the NPV calculation gives a different solution from that provided with the ROI calculation.

\[
\text{NPV}(AV - A) = \varepsilon 202,839 \\
\text{NPV}(AV - B) = \varepsilon 163,419
\]

The presented example has some limitations. First, the calculation of the benefits does not include the trend of virus attacks, which clearly has a decreasing trend over recent years [6]. It also does not include the additional costs (administration work and other intangible costs) that arise in the case of a virus infection. Nevertheless, it provides an approximate qualitative estimation. The results are presented in Table 2.

### Table 2

<table>
<thead>
<tr>
<th>Solution</th>
<th>ROI</th>
<th>NPV</th>
<th>IRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>AV-A</td>
<td>203%</td>
<td>€202,839</td>
<td>178%</td>
</tr>
<tr>
<td>AV002DB</td>
<td>428%</td>
<td>€163,419</td>
<td>173%</td>
</tr>
</tbody>
</table>

The final comparison is done with a calculation of the IRR from Eq. (7). The IRR confirms the NPV results, and is in favour of AV-A.

\[
\text{IRR}(AV - A) = 178\% \\
\text{IRR}(AV - B) = 173\%
\]

4.5. Standard approach procedure

The previous sections have shown that the quantification of an ICT security investment for the provision of privacy and security in an organization’s information system is a rather complex task. The studies carried out introduced different tools and methods that build up the most promising procedure in the decision-making process of how much investment is required in order for the possible threats to be minimized. The first step is certainly an evaluation of the SLE and ALE that takes into account the asset value and the ARO. The next step is a calculation of the possible value of the ROSI with different investment values. The outcome of this calculation leads to a calculation of the known economic indicators, such as the ROI, the NPV and the IRR. The NPV of the investment required for a security provision with a value greater than zero guarantees that the investment is not introducing losses; however, without providing information about the time period for the returns. For a final solution we have to consider the IRR indicator, which usually confirms the findings obtained with the NPV calculation. Fig. 2 illustrates the procedure and the steps in quantifying the ICT security investment.

5. Conclusions

The analysis of the problem associated with determining the size of an investment in information security has led to the development of a standardized approach for quantifying the ICT investment for the prevention of cyber crime and other security threats. The approach is based on the application of tools and methods that have been used for the evaluation of organizational asset values and the vulnerability of the systems. This was later used in combination with known economic metrics for an assessment of the investments and the index of return. A combination of several economic indexes, such as ROI, NVP and IRR, is proposed to be part of the procedure, as no single index can answer the basic questions about the assessment of the optimal investment required for the prevention of security threats. The study and the result presented are based on several studied examples that clearly show that the complete picture of the required investment cost and the benefits arising from the used solution can be obtained through a procedure that takes into account multiple indexes. The key direction for future research is to develop a mathematical model for a standardized approach to quantifying the information-security investment.
that will result in a recommendation for choosing an optimal security solution.

References


Prof. Dr. Borka Jerman-Blazić received the MS in Electrical Engineering from the University of Ljubljana and the Ph.D. degree in Natural and Computing Sciences from the University of Zagreb. Prof. Dr. Borka Jerman-Blazić is a Full Professor at the University of Ljubljana, Department of Economics and is the Head of the Laboratory for Open Systems and Networks at Jožef Stefan Institute. She teaches undergraduate courses in electronic communications and information security and postgraduate courses in Telecommunication Services and Technologies, Legal aspects and standards in ICT and E-commerce. Prof. Dr. Borka Jerman-Blazić is a member of the IEEE Computer Society, a member of the ACM, member of the New York Academy of Science since 1991, and a member of IFIP. She is appointed member to UNECE/CEFACT UN (Economic Commission for Europe) group for Internet enterprise development, appointed member of eTEN management committee of EU and a member of EU FP7 Programming Committee on Security, Chair (2004–2007) of the Internet Society of Europe (www.isoe-ecc.org), Distinguished Member of Slovene Society for Informatics, member of the editorial board of the International Journal of Technology Enhanced e-Learning. She received the Plaque of Appreciation of the Thai branch of IFIP and ACM for her services in Internet development and awards for best papers (IARIA IEEE conference). Prof. Dr. Borka Jerman-Blazić has been involved in more than 150 international conferences and workshops as a speaker, invited speaker and chair or a member of the programming committees. She has published more than 90 papers in refereed scientific journals, 154 communications on scientific meetings, 15 chapters in scientific books, 6 books and other 142 scientific contributions. She also has experience in editorship from books published by Kluwer PC and IOS Press (2001–2004).

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