TEST Engineering & Management

July-August 2020
ISSN: 0193-4120 Page No. 4984 - 4989

Models Evaluating Security Management in Investment Parameter

Dr. Sc. Tech. Hazir Hajdari
Computer and Telecomunications Science
Board Member RAEPC Kosovo

Co – Author: **Prof. Ass. Dr. Besnik Hajdari**
University of Mitrovica "Isa Boletini"
Faculty of Mechanical and Computer Engineering
E-mail: besnik.hajdari@umib.net

Article Info
Volume 83
Page Number: 4984 - 4989
Publication Issue:
July - August 2020

Article History
***Article Received**: 25 April 2020*
***Revised**: 29 May 2020*
***Accepted**: 20 June 2020*
***Publication**: 10 August 2020*

Abstract

The more companies base their activities on IT systems, the more the value of IT infrastructure and information becomes crucial. Companies try to objectify their investments on IS by calculating levels of required investments based on budget and Return on Security Investment (ROSI). The aim of this paper is to present some traditional, new and applied models of ROSI evaluations and their considerations.

1. Introduction

Since every company relies on IT infrastructure to communicate with clients, suppliers, economic institutions and other third parties, Information Security has been growing as a major concern. Security is generally categorized as protecting the confidentiality, integrity, availability, authentication and accountability[1] of information. Information Security is a whole system issue including software, hardware, physical environment, personnel, corporate and legal structures – a mosaic of science, technology, engineering and human factors[2]. Since information and Information Technology infrastructureconstitute a crucial asset to companies both in the private and public sector, its' leak, damage or manipulation comes with high tangible and intangible costs. Thus, for decades now companies are investing in Information Security (IS) partially motivated by fear of loss and environment pressure and partially by own strategic view.

Since when companies have started investing in IS, many questions have arose: (1)how much should companies spend on IS based on their budgets, (2) how to measure which IS solution to choose, (3) what do companies gain from IS investments? Usually, companies tend to consider IS as a cost/expense driven activity that has direct impact on organizations profitability [2] rather than an investment that will bring profits. Consequently, managers require that IS investments represent a balance between security and business requirements [3]. Moreover, managers require monetary evidence to support IS investments – they need to know how much will the investments pay back. To measure this payback many papers, models and analyses have been conducted on the concept of Return on Security Investment (ROSI).

The aim of this paper is to present the best-known and the most discussed works, models and papers on ROSI evaluation. To achieve this, we have chosen the first and most cited papers on ROSI, the newest and more evolving ones as well as real implemented and tested models published by celebrated companies that operate in the IT sector.

2. ROSI models and evaluations

For decades, there have been attempts to standardize models to assess ROSI. Traditional calculations used to measure ROSI were complex and cumbersome due to the many "soft figures" included in them[4]. The nowadays approaches tend to be more determined and focused on brute data. Before reaching the concept of ROSI, a long debate concerns the advisable amount to invest on Information Security, which we discus below.

2.1. Determining investments on IS

According to the senior controllers participating in the study described in[5], the primary target of the companies is to deliver highest possible total shareholder returns. Since, IS investments come with costs and expenses the natural attitude of companies is to consider with caution these expenses, solicitstrong evidence, justifications and monetary explanations in order to decide how much to invest on IS.

One of the most cited and discussed article on this topic is presented by Gordon and Loeb. This article aims to derive an economic model based on optimization that defines the optimal amount to invest in information security. The authors describe the amount to spent on the protection of an information set (that can take many forms: list of customers, an accounts payable ledger, a strategic plan, or company website) which is characterized by four parameters:

1. λ – represents the monetary loss to the firm caused by a breach of security of the information set,
2. t – represents the probability of a threat occurring ($0<t<1$),
3. v – represents the vulnerability, defined in the model as the probability that a threat once realized (i.e., an attack) would be successful ($0<v<1$),
4. z – represents the monetary investment in security to protect the given information set.

The authors make the assumption that the firms can influence the vulnerability (v) of information set by investing in information security, but the firm cannot invest to reduce the threat (t) – thus, since the threat probability is held constant, for notational simplicity they define:

$$L=t\lambda$$

where L represents the potential loss associated with the information set. As well, the authors denote S(z, v) as the probability that information set with vulnerability v will be breached, conditional on the realization of a threat and given that the firm has made an information security investment of z to protect the information.

The expected benefits of an investment in information security, denoted as EBIS, are equal to the reduction in the firm's expected loss attributable to the extra security. That is:

$$EBIS(z)=[v-S(z,v)]L$$

The expected net benefits from an investment in information security denoted ENBIS equal EBIS less the cost of investment:

$$ENBIS(z)=[v-S(z,v)]L-z$$

The optimal investment, z*, is reached where ENBIS function value is maximized. The analyses show that the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less than 37%)[6].

2.2. Quantitative ROSI evaluations

2.2.1. ROSI based on ALE

Since security is more about loss prevention than gain of profits, the quantitative assessment of ROSI is done by calculating how much loss is avoided thanks to the solution – the below variables are presented[7]:

1. Single Loss Expectancy (SLE) - The SLE is the expected amount of money that will be lost when a risk occurs. In this approach, SLE can be considered as the total cost of an incident assuming its single occurrence.
2. Annual Rate of Occurrence (ARO) - The ARO is a measure of the probability that a risk occurs in a year.
3. Annual Loss Expectancy (ALE) - The ALE is the annual monetary loss that can be expected from a specific risk on a specific asset. It is calculated as follow:

$$ALE=ARO*SLE$$

Analyses show that the more a solution is effective the more reduced is the ALE. This monetary loss reduction can be defined by the difference of the ALE without the security solution versus the modified ALE (mALE) implementing the security solution:

$$\text{ROSI} = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

This also equals to the mitigation ratio of the solution applied to the ALE:

$$\text{ROSI} = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

Although the proposed model presents as a result a raw value, disadvantages of this evaluation model are that the result comes as a conclusion to many approximations. Actually, coming up with meaningful values for the factors in the ROSI equation is no simple task[8] particularly about determining the ratio of risk mitigation. However in [8] are proposed the below justifications and advises:

1. With a good survey and scoring system for productivity, combined with external measurements of intellectual property value, it becomes possible to quantify risk exposure in a repeatable and consistent manner.
2. Even with an inaccurate scoring algorithm, using a scored assessment as a method of determining risk mitigation is effective because the scores are repeatable and consistent, and therefore can be used to compare the ROSI of different security solutions.

In addition to the ALE model, a proposal that comes from other ROSI evaluations of non-revenue generating programs is the KPI model which uses indicators (regarding human factor, information or infrastructure vulnerability etc.) to represent changes in the organization caused by the investment[9].

2.2.2. ROSI based on costs

Al-Humaigani and Dunn describe a quantitative assessment to produce robust ROSI numbers based on the derivation that the point of maximum return on security investment is where the total cost of security is lowest, including both the cost of security breaches and the cost of the security controls designed to prevent them. The model is used when different solutions are compared. The model is to use elements pertaining to[3]:

1. What it costs to invest in Information Security spending?
2. What it costs not to invest in Information Security spending?

The authors identify the below listed costs, as elements needed for every security control system or solution:

1. CT1: The cost of procuring the security tool or software, its licenses, and upgrades.
2. CT2: The cost of the extra physical hardware, rooms, and facilities needed.
3. CT3: The cost of the training and the time of the human resources forcing the security policies and implementing the security tool.
4. CT4: The losses due to the limitations placed on the business and the users.

5. CT5: The cost of adopting secured-by-design strategy while designing network infrastructure, configuration of operating systems and databases, or application development.
6. CT6: The financial cost of items, equipment, facilities, or systems in order to recover from a security incident /threat.
7. CT7: The losses due to business interruption.
8. CT8: The losses in human casualties or injuries.
9. CT9: The losses in loss of data from business and legal aspects.
10. CT10: The losses in the reputation and goodwill.
11. CT11: The amount that the insurance pays due to the loss caused during an incident.
12. KT: The probability of the security incident/breach to happen (without implementing any security control system /solution).

Thus, the return on investment of every security control system/solution becomes:

$$\text{ROSI} = \sum[K_T(C_{T6} + C_{T7} + C_{T8} + C_{T9} + C_{T10}) + C_{T11} - (C_{T1} + C_{T2} + C_{T3} + C_{T4} + C_{T5})]$$

and the chosen solution must have the highest ROSI.

2.2.3. ROSI based on game theory

Game theory is used to analyze problems in which the payoffs to players depend on the interaction between players' strategies. For example, in the IT security investment problem, the firm and the hackers are players. The firm's payoff from security investment depends on the extent of hacking it is subjected to. The hacker's payoff from hacking depends on the likelihood he or she will be caught. Thus, the likelihood of the firm getting hacked depends on the likelihood the hacker will be caught, which, in turn, depends on the level of investment the firm makes in IT security. The first step in using game theory to analyze such strategic interactions among players is to develop a game tree that depicts the strategies of players[10]. Then is needed the evaluation of probabilities of reaction till is reached the stable point strategy. The model is described in the Cavusoglu, Mishra and Rachunathan paper.

2.2.4. ROSI based on Security Management Solutions

As executives tried to navigate the new requirement for ROSI, they began to consider viewing Security Management Solutions in three categories, each of which provide incrementally more tangible Return on Investment (ROI):

1. Effective security
2. Risk reduction
3. Business efficiency that transcends security

To make the process of articulating ROSI easier, security professionals looked for new easier ways to make a convincing case for the investments they needed to deliver proper Security Management Solutions. One of the options was viewing Security Management Solutions in categories. Three categories emerged, with their differences delineated by the scope and impact a solution provides to an organization. The categories can be outlined as follows:

1. Solutions that provide security effectiveness
2. Solutions that reduce risk
3. Solutions that deliver business efficiency

Each level provides specific benefits to the organization. Those benefits can be mapped to ROSI as described by Holoman and Kuzmeskus[4].

2.2.5. ROSI based on Visualization of Financial Implications

This method described by Brocke, Buddendick and Strauch is based on the calculation of cash flow of companies based on their expenses on implementing the security solutions and incomes. All relevant in-

and out-payments have to be consolidated to one cash flow series. In addition, the reduced expected loss has to be taken into account. In a separate table the series of payments without the investment (without- case), should be aggregated. The series of payments is transferred to the VOFI. A VOFI is a collection of all relevant payments in one spreadsheet.
The balance on financial investment of the last period is the terminal value of the investment. This value should be compared to all terminal values of the VOFIs alternatives.The net terminal value of the investment is the difference between the terminal value of the investment and the terminal value of the opportunity (the second-best solution). The investment should be realized when the net terminal value is positive[11].

2.2.6. ROSI of INTEL

Intel IT developed a model for measuring return on security investment (ROSI) in their manufacturing environments.Their ROSI approach is based on actual incident data trending rather than on an assessment of potential exposures and vulnerabilities.Because the model measures the reduction in incidents, it can be applied only to security programs designed to reduce the number of incidents, but not to security programs that reduce the effects of incidents.

INTEL's ROSI methodology involves several steps:

1. Evaluating cyber-attack incident data averages over time.
2. Measuring the reduction of incidents from implementing new security programs.
3. Valuating the impact of avoided incidents.

Then they apply the results to similar areas to estimate future value[12].

2.2.7. ROSI based on strategic value

Businesses often focus on the short term ROI and neglect the strategic value if IS investments. As it was introduced by Locher, the risk analysis is performed best top-down scenario oriented, e.g. business units have to quantify costs of unavailability in dependence on the duration, costs of loss of confidentiality, while the IS department must quantify costs of loss of integrity and the probability of these security issues. This results in the business impact of security risks and allows determining the influence of security on the necessary regulatory capital charge and the expected losses. Based upon this data, a security manager is able to work out a security plan bottom-up[13].

3. Conclusions

As vulnerabilities increase, business leaders must understand, anticipate and manage information security as a business priority[14]. Companies both in the public and private sector are trying to monetarize their investments in IS and moreover, they are counting on ROSI to justify and decide for their actions. An economics perspective naturally recognizes that while some investment in information security is good, more security is not always worth the cost[6] – the value of the asset always should overcome the expenditure on its' investment.

There are many ways of calculating ROSI based on optimization, comparison and managerial perspective. Companies can choose one or more alternative models to calculate the ROSI for their solutions, based on the type of information they posses, the analytical experience of the staff and the tools they own and then compare the results. Experience has shown that financial evaluations of IS investments fail, not because the models proposed are problematic but because they are conduced improperly, with lack of professionalism and devotion.

Bibliography

[1] A. Vorster and L. Labuschagne, "A framework for comparing different information security risk analysis methodologies," in *ACM International Conference Proceeding Series*, 2005.

[2] T. K. Tsiakis and G. D. Pekos, "Analysing and determining Return on Investment for Information Security," in *International Conference on Applied Economics – ICOAE*, 2008.

[3] M. Al-Humaigani and D. Dunn, "A model of

return on investment for information systems security".

[4] K. Holoman and A. Kuzmeskus, "The Evolution of Return on Security Investment (ROSI)," Schneider Electric Integrated Security Solutions, 2012.

[5] C. Magnusson, J. Molvidsson and S. Zetterqvist, "Value creation and Return On Security Investments (ROSI)".

[6] L. Gordon and M. Loeb, "The economics of Information Security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, p. 438–457, 2002.

[7] European Network and Information Security Agency, "Introduction to Return on Security Investment," 2012.

[8] W. Sonnenreich, "Return On Security Investment (ROSI): A Practical Quantitative Model".

[9] J. Stuntz, "A review of return on investment for cybersecurity".

[10] H. Cavusoglu, B. Mishra and S. Rachunathan, "A model for evaluating IT security investments," *Communication of the ACM*, vol. 47, no. 7, pp. 87-92, 2004.

[11] J. Brocke, C. Buddendick and G. Strauch, "Return on Security Investments - Design principles of measurement systems based on capital budgeting," in *Americas Conference on Information Systems (AMCIS)*, 2007.

[12] Intel Information Technology, "Measuring the Return on IT Security Investments," 2007.

[13] C. Locher, "Methodologies for Evaluating Information Security Investments - What Basel II can change in the financial industry," in *European Conference on Information Systems (ECIS)*, 2005.

[14] E. Karofsky, "Insight into return on security investment," *http://techupdate.zdnet.com/techupdate/stories/main/0. 141 79,2878550.00.html*, 2002.

[15] Goverment Chief Information Office, "A Guide for Government Agencies Calculating Return on Security Investment," Lockstep Consulting, 2004.