Value creation and Return On Security Investments (ROSI)

Christer Magnusson, Josef Molvidsson and Sven Zetterqvist
Department of Computer and System Sciences
Stockholm University/Royal Institute of Technology
Forum 100, SE-164 40 Kista, Sweden
Tel: +46 (0)8 674 72 37
Fax: +46 (0)8 703 90 25
E-mail: cmagnus@dsv.su.se

Abstract. This paper investigates if IT security is as a part of value creation. The first part of the commentary focuses on the current theoretical conditions for IT security as a part of value creation. Different Return On Security Investment (ROSI) models are studied to investigate if they can calculate value creation with regard either to efficiency or to effectiveness. The second part of the paper investigates empirical evidence of a ROSI or any indication of a shareholder value perspective on IT security in three large, listed companies from different business segments. What they have in common is their first priority: value creation. The commentary begins by describing the "Productivity Paradox". It is followed by the most well-known ROSI models. Then, it explains the models applicability in value creation. Next, the three companies in the study are investigated. In the following section conclusions are drawn. Finally, the results of the research are discussed.

1 Introduction

To promote shareholder value every measure taken by the management should maximize value creation, from strategic investments to procedures for managing the daily operations. Since a cornerstone in shareholder value is free cash flow, "...the underlying value drivers of the business must also be the drivers of free cash flow" [1]. No other strategies are accepted than those linked to the creation of shareholder value:

"Value based strategic planning upholds no particular orthodoxy. For instance, if more market share, more customer service, more quality, or re-engineering the manufacturing process to increase efficiency will create more value for the business, it is a good thing. If the effort does not create

Please use the following format when citing this chapter:

Magnusson, C., Molvidsson, J. and Zetterqvist, S., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 25–35.

higher value, further investment in share, service or quality is unjustified". [2].

According to this principle, Net Present Value (NPV) calculations for IT security investments should be drawn up to "compete" with other investments on the same conditions and to be a part of the value creation. The first objective of this study is to investigate the current theoretical conditions for IT security as a part of the value creation. Secondly, we are interested in finding out the empirical indications of a shareholder value perspective on IT security. Finally, conclusions are drawn.

This paper is directed towards researchers and practitioners in the field of security and risk management. However, the commentary may also interest Chief Financial Officers, controllers, line managers, and providers of security products and services.

The commentary begins by describing the "Productivity Paradox". It is followed by the most well-known ROSI models. Then, it explains the models applicability in value creation. Next, the three companies in the study are investigated. In the following section conclusions are drawn. Finally, the results of the research are discussed.

2 Methodology

In order to start reasoning on how IT security could be managed more rationally as an investment category, it should be investigated how the category is being used today. Our ambition is to elucidate this. In order to make the area comprehensible, we will start with "The Productivity Paradox", which will provide the necessary basis before we continue going through different models for "Return On Security Investments" (ROSI) and to try to assess their applicability. We will then make an empirical study on security investments.

In the empirical study we are interested in finding out if security investments are an integrated part in value creation, or at least calculated, or if they are decided on without estimating their financial value? We approached three subjectively chosen companies to try to find, if not an answer, at least an indication of answer to these questions. A prerequisite for the participation in the study was that the company in question was listed at a stock exchange, since we then could assume that it had a shareholder value perspective on value creation. Moreover, the company should be in different business segments to reduce the risk with segments specific behavior.

3 The Productivity Paradox

There are at least two ways IT security can create business value:

Firstly, it can increase a company's efficiency. This means a company will decrease operational expenses due to investments in IT security. A security service (or product), for example, will execute controls, previously carried out by back office personnel, thus increasing back office productivity. IT security investments can also increase efficiency by reducing costs for business interruption, fraud, embezzlement,

etc. Secondly, IT security can increase a company's effectiveness. This means that IT security functionality will enable new, superior products or processes, thus providing a competitive advantage in the market. Banks, insurance services and air carriers with reengineered business models, completely based on Internet, are examples of businesses were IT security is a business enabler; without security these services would not sustain Internet hostilities [3, 4].

The major problems with IT security investments is however often the difficulty to identify and quantify its benefit, especially to translate it into economic terms and thus show its potential profitability [5, 6].

The problem to motivate IT security investments economically, is partly a consequence of the difficulties to generally produce correct calculations for IT investments, compared to traditional investments. Reasons for this are:

- The lack of a uniform working method to establish profitability
- IT investments will often carry their expenses, but not their benefits
- The general difficulty to identify and quantify the yield of IT investments

This originates in an "unjust" picture of IT projects; they bear all of their expenses, since these are easily quantified, but may not include their benefit, since these "cannot be identified". The noted economist Robert Solow quipped that computers are everywhere - except in "the productivity statistics" [7], and the economic historian Paul A. David invented "The Modern Productive Paradox" (Robert Solow) to describe the phenomenon. The Productive Paradox indicates the experienced loss of a positive correlation between investments in IT and an improvement of the companies' productivity due to these investments [8]. In 1996, a Swedish study established, that it was a paradox that there were almost no economical models to calculate the *benefit* from IT, although IT investments amount to several per cents of Sweden's BNP [8]. For some time now some attempt has been made to calculate the benefit from IT security. This will be studied more closely in the following sections.

4 Return On Security Investments

The investment category IT security inherits many of the problems which arise when valuating IT investments, but has also its "own" problems, e.g.

- How can the argument be overcome that security investments do not generate any revenue?
- How can an IT security investment be established as cost-effective, when the best that could happen is that "nothing" happens
- How can the optimal level of the total IT security investments be determined

A number of attempts have been made to adapt the existing economic profitability models to the special requirements for IT security in order to value IT security correctly. This kind of models was only recently developed. They have been

able to quantify the earning capacity from IT security investments on a more scientific basis instead of merely "listing" the various abstract benefit from these investments.

ROSI is an acronym for Return On Security Investments, referring to research results from different directions in the US. It is however emphasized that this research is more or less in its infancy. The results published so far are however starting to gain acceptance in the academic world and to some extant also within the trade and industry.

The problem that the ROSI models are trying to bridge is the validity on, or even the lack of, statistics and data on various security incidents and attacks. When there is no information available showing what can be regarded as for example an extreme or medium number of attacks of a certain kind, it will be very difficult for different actors to assess their optimal level of security. One cannot ask oneself the question "are we in a good position" or "what does it mean for us if we would invest another million in security".

The quality of statistics on information security incidents has been criticized. Even Computer Security Institute (CSI) admits that their annual reports on data related crime were not done scientifically, but only intended to give a hint on the situation and the very best they could do in the present situation [9].

4.1 The Hummer model

Under the management of Hua Qiang Wei [10] a scientific team from the University of Idaho has developed the Hummer model. It consists principally of a "box", which in a network logs suspected incoming traffic which has passed through a firewall. To establish what can be regarded as "suspected" traffic, certain special patterns are stored. When an attack is suspected, reports will be sent to the administrative staff who can investigate the matter.

The model shows that it is more cost-efficient to discover and handle attacks using intrusion detection systems than using other preventive IT security mechanisms. Questions that the scientific team had to decide on with regards to costs and profitability were to try to establish the costs to discover an incident, the operational security costs and financial consequences if an attack would remain undiscovered.

To carry out this valuation the work was initiated by valuing the assets that could be reached through the network. Software could be valued in the same way as information. The valuation was also graded to define that, e.g. information A was three times as valuable as information B. Then different forms of attacks are associated with different costs in accordance with the standard of the U.S. Department of Defense.

In that way the ratio Annual Loss Expectancy (ALE) could be calculated in accordance with the normal procedure as a measure of the economic damage an attack causes multiplied with its likeliness. Consequently, an attack that would cost 100.000 dollar and occur every second year has an ALE of 50.000 dollar.

Accordingly, the Hummer model uses the ratio ALE as an important component when valuating intrusion detection systems. According to Wei the economic basis of

the Hummer model is a "cost-benefit analysis", the objective of which is to weigh the pro and cons of intrusion detection systems with one another.

4.2 The Hoover model

The Hoover model has been developed by the Massachusetts Institute of Technology and the company @Stake in Boston, U.S., under the management of Kevin Soo Hoo [11]. The model's foremost objective is to calculate how companies who develop software can achieve the maximum yield on their security functionality investments. Hoover is principally database managing detailed information on security problems and vulnerabilities in software. The information has been obtained from companies that develop software and participated in the research work trying to understand how they could develop their products with a higher security level.

To be able to calculate yield due to IT security functionality investment in the different programming development processes one starts, for example, from the motto "A one dollar investment to manage a bug in the designing process will save 99 dollar compared to managing a bug later in the implementation phase".

The Hoover model's most important aspect from the historic information in the database is that the earlier one includes security into the software process, the higher the yield. The general result that the model generates is that security functionality investment in the designing phase results in the highest yield, 21 per cent. To add security functionality later in the development phase lower the yield, 15 per cent in the implementation phase and 12 per cent in the testing phase.

The Hoover model illustrates thus two ordinary construction mistakes in the development of software: to include security functionality "at last minute" and to let the users (or hackers) discover the security problems before one takes (tries to take) measures to correct these. The model shows that the earlier security aspects are considered in the development phase, the higher is the yield. The model shows this by applying Net Present Value (NPV) based calculations [11].

4.3 The CMU model

This quantitative study by Carnegie Mellon University shows how a system's ability to survive attacks increases if investment increases; it shows when the optimal investment level takes shape.

The study is primarily a regression analysis on "attack data" obtained from CERT [12]. The CMU model managed data between 1988 and 1995. It investigated which attacks occurred and how often, the odds for a certain type of attack affecting a certain company, the caused damage and the available defense including functionality [13].

This data was utilized to develop a model that could generate attacks in simulated companies. Consequently, one could get a picture of the frequency and grade of seriousness in the different attacks in practical terms. Afterwards the reaction of different networks was studied, during the attack and under various conditions. For instance, the grade of security (grade of cost) and the probability for attacks were varied to learn how these would affect the ability to resist attacks.

The absence of a "binomial view" on security was one of the news in the CMU model. The model no longer presumed that a company would be either attacked or not, but introduced a scale on how many times a company had been attacked. The systems ability to resist the attack (survivability) was measured between 0 and 1; 0 signified that the company was completely "eliminated" by an attack and 1 that the company remained completely unaffected by an attack.

By plotting data from these simulations, a model of the system's ability to survive depending on the security investment costs could be obtained. The cost was calculated in absolute terms ($) and the grade of survival between 0 and 1. The regression line shows a connection that is strongly increasing for low costs, but decreasing for high costs. Consequently, there is a decreasing marginal benefit when increasing the cost for security investments.

Accordingly, the CMU model can establish that the yield that can be delivered by security investments will be the highest in the initial stage and then gradually decrease when more money is invested in security.

By combining an imaginary curve, representing yield, with a curve representing the benefit that a company experiences due to increased security investments, the "optimal security" can be identified by using the CMU model. It is depicted in the diagram when the two curves intersect.

The CMU model concludes that if one can proof the need for a security investment, the model can deliver optimal security.

5 Applicability in Value Creation

It is important to observe that the three ROSI models studied are to a different extent "economically correct" with regard to the valuation of IT security. Their most important contribution is to formulate practical procedures how IT security investments may be evaluated. However, it can be noted that the basic economic models, which have been used, are not always explicitly specified.

With regard to the Hummer model it can be noted that the advantage of using an intrusion detection system is calculated by deducting the generated reduction in ALE from the annual cost for the system. The asset valuation, which the ALE calculation is based on, is done by using the present (capitalized) value. The model takes also as one's starting point that certain assets are more difficult to value in monetary terms than others. That is the reason why the company's assets are divided into "tangible assets" (principally physical assets as working stations and servers) and "intangible assets" (principally assets as stored data and information). It is only the first category that can be valued in economic terms. The value of the latter asset type is estimated in terms of "points" [10].

In the Hoover model Soo Hoo tries to calculate the benefit security functionality provides by using the function called "net benefit". The benefit is quantified in monetary terms. Soo Hoo points also out that the valuation of "intangibles" can generate controversial values. He tries therefore to consider this by only focusing on ALE. This value if calculated from relatively concrete losses in connection with the implementation of different security policies. According to Soo Hoo an investment

decision can often be made based on the relatively concrete consequences that can be estimated, since these are generally big enough to prove profitability in a potential security investment [9]. Finally, Soo Hoo calculates a "net benefit" consisting of ALE minus "added cost" plus "added profit". By "added cost" one refers to the cost that can arise because of introduced security functionality, e.g. the staff is dissatisfied with circumstantial security routines. "Added profit", on the other hand, represents new business opportunities (IT security effectiveness) because of the new security investments, e.g. increased customer trust after the implementation of a PKI system.

The CMU model is not primarily about producing a monetary measurement of the value in a security investment. The model focuses rather on measuring each company's individual risk aversion in order to determine the company's optimal grade of investment. The decision criterion for this model will be directly affected by the investments costs, but unlike other investments it will not directly be affected by the revenues or monetary profits from a security investment. It is rather the subjective benefit vs. the cost that arises.

After this further accounting of the ROSI models' economic basis it can be established that it is neither easy to verify whether the models claim to be economically correct, nor if they claim to develop a valuation model for ex post or ex ante perspective. A common feature of the models is that they all value advantage in terms of net benefit. This term cannot not without difficulty be translated into cash flows. Therefore it is difficult to establish to what degree the ROSI models could be utilized in a Net Present Value (NPV) or Return On Investment (ROI) calculation and accordingly in value creation.

6 The study

To be able to carry out our empirical study we needed some large, listed companies with different business portfolios but with one unifying objective – a clear focus on shareholder value. Three companies were chosen for and accepted to participate in the study. They have completely different business portfolios. One company is the global leader (based on revenue) in white goods. The second company is one of the largest banks (by volume) in the Nordic region. The third company is a major Nordic telecom operator (measured in revenue).

All three companies have strong balance sheets. However, all of them have experienced financial stress and the bear market. One of the companies was not far from bankruptcy in the beginning of the nineties. Another has seen its shares dropping substantially over the last years (even though currently it has recovered somewhat). The third company faced the challenge with integrations costs after massive acquisitions around the globe.

After we had studied the companies' annual reports, it became obvious that shareholder value is on the agenda in all three companies. This gave us the opportunity to find an answer to our second research question, i.e. if there are any empirical indications of a value creation perspective on IT security, at least in these companies? We put forward to following questions to the companies.

- Do you have internal measures for controlling value creation?

- What is your business' appetite for risk?
- What internal measures do you have for controlling the IT risks, as for example the ROSI formulas?

The questions mentioned above were discussed with senior controllers on Group level in each corporation. Their positions were "Head of Group Controller and Finance" or "Head of Group Business Control". Even though they formally had slightly different positions, they had in common that they were responsible for overlooking the processes of value creation and investments in the companies.

6.1 Measures for controlling value creation

According to the senior controllers, the primary target of the companies is to deliver the highest possible shareholder returns (change in share price and dividends relative local market index or industry peer group). However, there were some differences in the methods for governing and controlling the business units in their effort to create shareholder value.

The bank had three value drivers for their business units: the key figure "Costs/Revenue" (excluding credit losses); Return On Equity (ROE); and a qualitative measure to estimate employee satisfaction. When being asked a question about the balance between the financial measures and the qualitative measure, the Senior Vice President made clear, that "the bottom line is always the most important".

The Telco had a concept named "Wanted Positions" covering customers, services, personnel, and growth (turnover and ROE). Priority number one was growth in turnover. The white goods giant had one single value driver: their internally developed version (Operative income – (Weighted Average Cost of Capital x Net assets)) of Economic Value Added. The Group Business Controller made it absolutely clear that the financial goals, expressed in the Groups value creation figures for the business units, were the first and only priority.

6.2 Risk appetite

A corporation can decide on its aggregated risk appetite and express it in percentage of some key figures, as for example:

- 1-5% on Working Capital
- 5-10% on Cash Flow
- 1-3% on EBITDA (Earnings Before Interest, Taxes, Depreciation, and Amortization)
- 3-5% on Earnings Per Share

The reasons behind deciding on risk key figures are twofold. Firstly, a corporation decides on a risk level estimated to sustain any impact on its share value due to incurred losses. Secondly, the figures allow the company to actively take on calculated risks and not to avoid them at any price.

None of the companies in the study had any financial key figures for IT risk appetite. All three companies had individual and aggregated credits limits for there customers and financial risk management systems. The Telco came closest to some

sort of (qualitative) key figure of risks with a list of 20 risks that could threaten the "Wanted Positions" for the Group. The controllers of the companies explained that the IT risk was not an integrated part of their value creation systems. Consequently, management of the IT risk had no impact on the bonus systems, either.

6.3 Measures for controlling risk

None of the companies' controllers had any knowledge of the three ROSI models, or of any other methods or models (quantitative or qualitative). The controller of the Telco thought that maybe locally, in the business units and subsidiaries, some kind of NPV calculation (or similar) was carried out. The others had not heard of any unit in their corporations that had made any calculation whatsoever of investments in security.

All of the controllers underlined that the reason for neither having focused on risk analyses nor made calculations on IT security investments was that risk costs were not a part of their companies' value creation (and bonus) systems.

7 Conclusion

The first objective in this study was to investigate the current theoretical conditions for IT security to become a part of value creation. The ROSI models in our study are of limited value to help us calculate value creation neither with regard to efficiency nor to effectiveness. A fundamental reason is that the basic economic models, which were used, are not stated explicitly. This reduces obviously their practical usefulness.

Moreover, it is neither easy to verify whether the models claim to be economically correct, not if they claim to develop a value model for ex post or ex ante perspective. One further difficulty to apply the models is that they all value advantage in terms of net benefit. This concept cannot be easily transformed into cash flow. Therefore, it is not easy to establish to what degree the ROSI models' result could be utilized in a NPV or ROI calculation and accordingly in value creation. These difficulties may be a reason for the result in our empiric study.

According to the senior controllers participating in the study, the primary target of the companies is to deliver highest possible total shareholder returns. Despite that, made the result of the study it absolutely clear that there are no empirical evidence what so ever of a shareholder value perspective on IT security in these companies; there are no models in place for calculation the value contribution of IT security investments. As a matter of fact, there aren't any calculations done at all (at least not that the senior controllers are aware of).

8 Discussion

Straub et. al. in [14] discussed (information) security as "back-burner issue" for managers as well as employees, and the difficulties to change such a perception.

Sherwood et. al. [15] concluded that "[IT] Security has a bad reputation for getting in the way of real business". A study conducted by Nalla et. al. [16], underlined that the need for management and communication skills is critical to the security function.

A question arises why don't IT risk and security managers take the opportunity to integrate their work tasks with value creation and get senior management attention? Is it possible that Angell's "pathology of consciousness" in [17] gives an explanation; are they trapped within a mode of the traditional social organization (the IT security community) where the (traditional technology oriented security) assignments are created and supported in their everyday lives?

Another question may be if the IT risk and security managers are qualified enough in general management to be aware of the drivers behind value creation. Without these qualifications, it is difficult to navigate with the IT security and risk management function; the risk the IT security profession runs is to be left behind in the corporate world of yesterday.

Nevertheless, one thing we know is that cost for IT security is increasing; according to a CSI/FBI survey, 34% of respondents said security accounted for more than 5% of their organizations' total IT budgets and 13% spent more than 10% [18]. Another thing we know is that increasing cost is usually a reliable way to get senior management attention. Then, IT security may go the same route as many costly IT projects – the outsourcing and offshore route. The value creation in such a context is fairly easy to calculate.

Acknowledgement

We would like to take this opportunity to express our gratitude to the Executive Management in the companies who gave us this opportunity to gain some insight in value creation in their companies. We are especially grateful to the Chief Security Officers for their support during the project.

The opinions expressed in this paper are the author's opinions and do not necessarily represent the views of the companies in the study.

References

1. T. Copeland, T. Koller, and J. Murrin, Valuation, Measuring and Managing the value of companies, second edition, McKinsey & Company, Inc. (John Wiley & Sons, Inc, 1995).
2. J. McTaggart, P. Kontes, M. Mankins, in: Shareholder Value, I. Cornelius and M. Davies (FT Financial Publishing, Pearson Professional Limited, London, 1997), p. 223.
3. C. Alberts and A. Dorofee, Managing Information Security Risks, The OCTAVE Approach, Carnegie Mellon Software Engineering Institute, USA (Addison Wesley, 2003).

4. A. Granova and J.H.P. Eloff, Who Carries The Risk? Proceedings of the 4TH Annual International Information Security South Africa conference, July 2004, (ISBN 1-86854-522-9).
5. B. V. Solms and R. V. Solms, The 10 deadly sins of information security management, in: Computers & Security, Vol.23 No 5 (ISSN 0167 –4048, 2004), pp. 371-376.
6. J.H.P. Eloff, Tactical level - an overview of the latest trends in risk analysis, certification, best practices and international standards, Information Security Architectures Workshop, Fribourg, Switzerland, February 2002.
7. P.A. David, The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox, (American Economic Review, 1990).
8. T. Falk and N-G. Olve, IT som strategisk resurs (Liber-Hermods, 1996).
9. K.J. Soo Hoo, How Much Is Enough? A Risk Management Approach to Computer Security, Ph.D. Thesis, University of Stanford, 2000.
10. H. Wei, D. Frinke, O. Carter, and C. Ritter Wei, Cost-Benefit Analysis for Network Intrusion Detection, Centre for Secure and Dependable Software, University of Idaho, Proceedings of the 28th Annual Computer Security Conference October, 2001.
11. K.J. Soo Hoo, A.W. Sudbury, A.R. Jaquith, Tangible ROI through Secure Software Engineering (Secure Business Quarterly, 4th Quarter 2001).
12. The CERT® Coordination Center (April 30, 2003); http://www.cert.org.
13. S.D. Moitra and S.L. Konda, A Simulation Model for Managing Survivability of Networked Information Systems, Technical Report CMU/SEI-2000-TR-020, Carnegie Mellon Software Engineering Institute, 2000.
14. D.W. Straub and R.J. Welke, Coping With Systems Risk: Security Planning Models for Management Decision Making (MIS Quarterly, December 1998).
15. J. Sherwood, A. Clark, A, and D. Lynas., Enterprise Security Architecture: a business driven approach (CMP Books, USA, 2005).
16. M. K. Nalla, K. Christian, M. Morash, and P. Schram, Practitioners' perceptions of graduate curriculum in security education (Security Journal, 6, 1995), pp. 93-99.
17. I. O. Angell, Computer security in these uncertain times: the need for a new approach, Proceedings of the Tent World Conference on Computer Security, Audit and Control, COMPSEC, London, UK, 1993, pp. 382-388.
18. Eleventh Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2006; www.gocsi.com.