Title: Adding value to business performance through cost benefit analyses of information security investments

Author: Lucas Cardholm

Thesis

Study programme in
Master of Business Administration in Marketing Management
Abstract / Summary

The purpose of this thesis is to present an approach for good practice with regards to using cost benefit analysis (CBA) as a value-adding activity in the information security investment process for large enterprises. The approach is supported by empirical data.

From a MIO model perspective, this report is focused on the phase of strategic choices regarding organization, i.e. trying to find optimal investments for efficient operations. To assess, improve and monitor the operational effectiveness and management’s internal control environment is essential in today’s business execution. Executive management and boards are increasingly looking for an information security governance framework that encompasses information technology and information security: a single framework through which all information assets and activities within the organisation can be governed, to provide the optimum capability for meeting the organisation’s objectives, in terms of functionality and security.

The investment decision is one of the most visible and controversial key decisions in an enterprise. Some projects are approved, others are bounced, and the rest enter the organisational equivalent of suspended animation with the dreaded request from the decision makers to “redo the business case” or “provide more information.”

The concept of cost benefit analyses of information security helps management to make decisions on which initiatives to fund with how much, as there needs to be an approach for measuring and comparing different alternatives and how they meet business objectives of the enterprise. Non-financial metrics are identified using different approaches: governance effectiveness, risk analysis, business case analysis or game theory. The financial performance metrics are driven by the main value disciplines of an enterprise. These lead to the use of formulas enabling the measurement of asset utilisation, profit or growth: ROI (ROIC), NPV, IRR (MIRR), FCF, DCF, Payback Period, TCO, TBO, EVA, and ROSI.

The author shows research in the field of good corporate governance and the investment approval process, as well as case studies from two multinational enterprises. The case from Motorola demonstrates how IT governance principles are equally applicable to information security governance, while the case from Ericsson demonstrates how an information security investment decision can be supported by performing a cost benefit analysis using traditional marketing approaches of business case analysis (BCA) and standard financial calculations.

The suggested good practice presented in this thesis is summarised in four steps:

1. Understand main rationale for the security investment
2. Identify stakeholders and strategic goals
3. Perform Cost Benefit Analysis (non-financial and financial performance metrics)
4. Validate that the results are relevant to stakeholders and strategic goals

DISCLAIMER
This report is intended for academic training only and should not be used for any other purposes. The contents are not to be considered legal or otherwise professional advice. No liability is taken, whatsoever, by the author.
## Contents

**BODY** ........................................................................................................................................ 4  
- **PURPOSE AND RESEARCH QUESTION** .............................................................................. 4  
- **INFORMATION SEARCH** ........................................................................................................ 4  
- **DISCLAIMER** ........................................................................................................................... 4  
- **THEORY** .................................................................................................................................. 5  
  - *The value of information and the need for protection* ......................................................... 5  
  - *Governance and Internal Controls Principles* ....................................................................... 6  
  - *The Investment Approval Process* ....................................................................................... 11  
  - *Non-financial Performance Metrics* .................................................................................. 13  
  - *Financial Performance Metrics* ....................................................................................... 18  
- **EMPIRICAL DATA** .................................................................................................................. 28  
  - *Governance Arrangements* ............................................................................................... 28  
  - *Case Study: Information Security Governance at Motorola* ........................................... 30  
  - *Case Study: Cost Benefit Analysis of Security Investment at Ericsson* ............................ 33  
- **ANALYSIS** .............................................................................................................................. 37  
  - *The Information Security Investment Process* ..................................................................... 37  
  - *Non-financial Performance Metrics* .................................................................................. 39  
  - *Financial Performance Metrics* ....................................................................................... 45  
  - *Validation of the CBA* ......................................................................................................... 47  
- **RECOMMENDATION** ............................................................................................................... 48  
  - *Suggested Good Practice for CBA of Information Security Investments* ....................... 49  
  - *Reflections* .......................................................................................................................... 52  
  - *Final Note* ............................................................................................................................. 53  
- **SOURCES** ................................................................................................................................ 54  
  - **PRINTED SOURCES** .......................................................................................................... 54  
  - **ONLINE SOURCES** .......................................................................................................... 56  
  - **ILLUSTRATIONS** ............................................................................................................... 58
PURPOSE AND RESEARCH QUESTION

The purpose of this thesis is to present an approach for good practice with regards to using cost benefit analysis as a value-adding activity in the information security investment process for large enterprises. The approach should be supported by empirical data.

The thesis will be valuable to information security professionals responsible for investments in information security and to suppliers of information security services or products who want to better meet the needs of the customer companies.

INFORMATION SEARCH

The information found in this report is collected from the mandatory course literature of this programme and sources on the Internet.

When using the Internet, the quality of sources used need to be verified. In order to minimise the risk of low-quality resources, the author has used a combination of aspects when considering including sources:

- Published by a University or an identified company/author
- Published in a relevant context
- The source refers to/discusses other sources or opponent opinions

This report has been structured and footnoted in accordance with the suggested template from University of Gävle (HiG) and Backman’s book on academic reporting.

DISCLAIMER

This report is intended for academic training only and should not be used for any other purposes. The contents are not to be considered legal or otherwise professional advice. No liability is taken, whatsoever, by the author.

---

1 Backman, Jarl, 1998.
THEORY

The MIO Model is used in marketing management. The model gives a holistic view on marketing by presenting a framework called The MIO Matrix. The matrix, developed by Eriksson, Hauer and Hultén, provides a framework for relevant perspectives and critical questions to address in different stages of the marketing process, i.e. the present situation, analysis of the future, strategic choices and campaigns. Throughout the matrix we find three interdependent aspects to be considered. These are the external factors (market), the positioning of our products or services (interaction) and internal factors (organization).  

The cost benefit analysis (CBA) is a value-adding activity in the information security investment process for large enterprises. If the CBA is well implemented, it not only addresses asset utilisation aspects, but also opens up for profitable business enablement and growth. From a MIO perspective, this report is focused on the phase of Strategic Choices regarding Organization, i.e. trying to find optimal investments for efficient operations.  

The MIO Matrix

The value of information and the need for protection

The organisational principles for managing information security and IT in large multinational companies presented in this report, are largely based on research from the Massachusetts Institute of Technology’s Sloan School of Management. Their research shows that although information has always been important in business enterprises, with current technological developments, the role and value of information has changed significantly in recent years. Information:  

- is increasingly easy to collect and digitize  
- has increasing importance in products and services  
- is very hard to value or price  
- has a decreasing half-life  
- has increasing risk exposure (e.g., security and privacy)  
- is a significant expense in most enterprises  

---

3 Ibid.  
These factors together make information and IT the least understood and most poorly utilised key asset in many enterprises.  

Information security governance is part of the infrastructure- and asset management of the enterprise. Shirley M. Hufstedler, member of the board of directors at Harman International Industries state “The rising tide of cybercrime and threats to critical information assets mandate that boards of directors and senior executives are fully engaged at the governance level to ensure the security and integrity of those resources.”

Governance and Internal Controls Principles

As enterprises work to improve the security of their workplace assets, the ability to execute company strategies will depend on the effectiveness with which they manage their infrastructure. In this context, infrastructure management solutions will help enterprises release capital to re-invest in the core business, improve overall operational effectiveness by reducing overhead expenditures, increase employee productivity through better infrastructure performance, and plan and execute security upgrades more effectively.

To assess, improve and monitor the operational effectiveness and management’s internal control environment is essential in today’s business execution. With an increasing rate of regulatory requirements, e.g. Sarbanes-Oxley Act of 2002 or the European 8th Directive, any investment made in governance structures or the internal control environment need not only meet these external requirements, but also to be dedicated to improving the performance of the enterprise in order to avoid having a negative impact on its business.

With the introduction of modern Enterprise Resource Planning (ERP) systems, to strengthen the enterprises financial control environments, came hidden and unplanned challenges from an infrastructure perspective. The most obvious challenges were for IT organizations. ERP implementation required the conversion and upgrade of marginally networked, proprietary, un-managed, and unreliable distributed client-server networks into highly reliable, commercial-quality, distributed computing platforms. A second challenge was that the financial insights of ERP solutions made infrastructure-related costs more visible, but not necessarily more controllable. Finally, and perhaps most importantly, managing the service relationship between infrastructure assets and employees plays a decisive role in driving productivity and controlling costs. Breakdowns in the service of infrastructure assets directly impact employee productivity, which impacts both revenue generation and profitability.

---

5 Ibid.
6 Information Technology Governance Institute, 2006
8 The Senate and House of Representatives of the United States of America, 2002
10 Ernst & Young, 2006. Accessed 2007-06-17
There are two complementary sides of corporate governance articulated by the OECD:\(^\text{12}\):

- **Behavioural side of corporate governance:**
  “Corporate governance encompasses the relationships and ensuing patterns of behaviour between different agents in a limited liability corporation; the way managers and shareholders but also employees, creditors, and communities interact with each other to form the strategy of the company”.

- **Normative side of corporate governance:**
  “Corporate governance also refers to the set of rules that frame these relationships and private behaviours, thus shaping corporate strategy formation. These can be the company law, securities regulation, listing requirements. But they may also be private, self-regulation.”

The Information Technology Governance Institute, ITGI, states “Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme. […]”\(^\text{13}\)

Executive management and boards are increasingly looking for an information security governance framework that encompasses information technology and information security: a single framework through which all information assets and activities within the organisation can be governed, to provide the optimum capability for meeting the organisation’s objectives, in terms of functionality and security. Information security governance is built into ITGI’s model for IT governance, as shown in the illustration below.\(^\text{14}\)

---


\(^\text{13}\) Information Technology Governance Institute, 2006

\(^\text{14}\) Poole, Vernon, 2006. Accessed 2007-06-09
The definition of IT governance used by the Massachusetts Institute of Technology’s Sloan School of Management is “Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT.” This definition of governance aims to capture the simplicity of corporate governance – decision rights and accountability – and its complexity – desirable behaviours that are different in every enterprise.\(^{15}\)

The professional services firm Gartner confirms this, as it states “IT governance specifies the decision making authority and accountability to encourage desirable behaviors in the use of IT. IT governance provides a framework in which the decisions made about IT issues are aligned with the overall business strategy and culture of the enterprise. Governance is about decision making per se—not about how the actions resulting from the decisions are executed. Governance is concerned with setting directions, establishing standards and principles, and prioritizing investments; management is concerned with execution.”\(^{16}\)

ITGI defines IT governance as “the leadership, organizational structures, and processes that ensure that the enterprise’s IT sustains and extends the enterprise’s strategies and objectives.” They additionally state that “While governance developments have primarily been driven by the need for the transparency of enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance.”\(^{17}\)

ITGI has created a specific report for board members on Information Security Governance within the context of the framework CobiT. It is a control model to meet the needs of IT governance and ensure the integrity of information and information systems. In the report ITGI stipulates five basic objectives for Information security governance. The five objectives with illustrative goals are presented in the table below.\(^{18}\)

<table>
<thead>
<tr>
<th>Basic Objective</th>
<th>Illustrative goals</th>
</tr>
</thead>
</table>
| 1. Strategic Alignment | It is often difficult to achieve the goal of strategic alignment of information security in support of organisational objectives. Consider the following goals:  
- Ensure transparency and understanding of IT security costs, benefits, strategies, policies and service levels.  
- Develop a common and comprehensive set of IT security policies.  
- Communicate the IT strategy, policies and control framework.  
- Enforce IT security policies.  
- Define security incidents in business impact terms.  
- Establish clarity on the business impact of risks to IT objectives and resources.  
- Establish IT continuity plan that supports business continuity plans. |
| 2. Risk Management | To manage and mitigate risks and reduce potential impacts on information assets to an acceptable level, consider the following goals:  
- Account for and protect all IT assets.  
- Establish and reduce the likelihood and impact of IT security risks.  
- Perform regular risk assessments with senior managers and key staff.  
- Permit access to critical and sensitive data only to authorised users.  
- Ensure critical and confidential information is withheld from those who should not have access to it.  
- Identify, monitor and report security vulnerabilities and incidents.  
- Develop IT continuity plans that can be executed and are tested and maintained. |

\(^{15}\) Weill, Peter and Jeanne W. Ross, 2004, p8.  
\(^{16}\) Dallas, Susan, Michael Bell, 2004.  
\(^{17}\) Information Technology Governance Institute, 2003, p7  
\(^{18}\) Information Technology Governance Institute, 2006, p26
### Basic Objective

| Illustrative goals                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Resource Management                                                                 | Information security knowledge and infrastructure should be used efficiently and effectively. Consider the following goals:  
  - Maintain the integrity of information and processing infrastructure.  
  - Account for and protect all IT assets.  
  - Ensure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.  
  - Ensure proper use and performance of the applications and technology solutions.                                                                                                                                                                                                                                                                                                                                                     |
| 4. Performance Measurement                                                                 | Measuring, monitoring and reporting on information security processes ensures that organisational objectives are achieved. Consider these example metrics:  
  - Number of incidents damaging reputation with the public  
  - Number of systems where security requirements are not met  
  - Time to grant, change and remove access privileges  
  - Number and type of suspected and actual access violations  
  - Number and type of malicious code prevented  
  - Number and type of security incidents  
  - Number and type of obsolete accounts  
  - Number of unauthorised IP addresses, ports and traffic types denied  
  - Number of access rights authorised, revoked, reset or changed                                                                                                                                                                                                                                                                                                                                 |
| 5. Value Delivery                                                                                                                               | Security investments should be optimised to support organisational objectives. Security activities consume resources. Optimal investment levels occur when strategic goals for security are achieved and an acceptable risk posture is attained by the organisation at the lowest possible cost. The following goals should be considered:  
  - Ensure automated business transactions and information exchanges can be trusted.  
  - Make sure that IT services are available as required.  
  - Minimise the probability of IT service interruption.  
  - Minimise the impact of security vulnerabilities and incidents.  
  - Ensure minimum business impact in the event of an IT service disruption or change.  
  - Establish cost-effective action plans for critical IT risks |
The Governance Arrangements Matrix, shown below, lists five interrelated IT decisions, where the IT Investment is the key decision connected with cost benefit analysis.20

- IT principles – Clarifying the business role of IT
- IT architecture – Defining integration and standardisation requirements
- IT infrastructure – Determining shared and enabling services
- Business application needs – Specifying the business need for IT applications
- IT investment and prioritization – Choosing which initiatives to fund with how much

<table>
<thead>
<tr>
<th>Domain Style</th>
<th>IT Principles</th>
<th>IT Architecture</th>
<th>IT Infrastructure Strategies</th>
<th>Business Application Needs</th>
<th>IT Investment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Monarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Monarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feudal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duopoly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anarchy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t Know</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Governance Arrangements Matrix

Depending on the implementation of decision structures in the enterprise, the Governance Arrangements Matrix shows what archetype of governance arrangements exist for information security or IT. The table below explain the different archetypes for governance:21

<table>
<thead>
<tr>
<th>Archetype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Monarchy</td>
<td>Top management of the enterprise</td>
</tr>
<tr>
<td>IT Monarchy</td>
<td>IT specialists</td>
</tr>
<tr>
<td>Feudal</td>
<td>Each business unit makes independent choices</td>
</tr>
<tr>
<td>Federal</td>
<td>Combination of the group functions and the business units with or without IT involved</td>
</tr>
<tr>
<td>IT Duopoly</td>
<td>IT group and one other group (i.e. top management or business unit leaders)</td>
</tr>
<tr>
<td>Anarchy</td>
<td>Isolated individual or small group decision making</td>
</tr>
</tbody>
</table>

20 Ibid., pp10-11.
21 Ibid., pp54-55.
The table below illustrate the five key decisions in the matrix.\textsuperscript{22}

<table>
<thead>
<tr>
<th>IT key decision</th>
<th>Questions to address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT principles</td>
<td>1. What is the enterprise’s operating model</td>
</tr>
<tr>
<td></td>
<td>2. What is the role of IT in the business?</td>
</tr>
<tr>
<td></td>
<td>3. What are the IT-desirable behaviours?</td>
</tr>
<tr>
<td></td>
<td>4. How will IT be funded?</td>
</tr>
<tr>
<td>IT architecture</td>
<td>1. What are the core business processes of the enterprise? How are they related?</td>
</tr>
<tr>
<td></td>
<td>2. What information drives these core processes? How must the data be integrated?</td>
</tr>
<tr>
<td></td>
<td>3. What technical capabilities should be standardised enterprise-wide to support IT efficiencies and facilitate process standardisation and integration?</td>
</tr>
<tr>
<td></td>
<td>4. What activities must be standardised enterprise-wide to support data integration?</td>
</tr>
<tr>
<td></td>
<td>5. What technology choices will guide the enterprise’s approach to IT initiatives?</td>
</tr>
<tr>
<td>IT infrastructure</td>
<td>1. What infrastructure services are most critical to achieving the enterprise’s strategic objectives?</td>
</tr>
<tr>
<td></td>
<td>2. For each capability cluster, what infrastructure services should be implemented enterprise-wide and what are the service-level requirements of those services?</td>
</tr>
<tr>
<td></td>
<td>3. How should infrastructure services be priced?</td>
</tr>
<tr>
<td></td>
<td>4. What is the plan for keeping underlying technologies up to date?</td>
</tr>
<tr>
<td></td>
<td>5. What infrastructure services should be outsourced?</td>
</tr>
<tr>
<td>Business application needs</td>
<td>1. What are the market and business process opportunities for new business applications?</td>
</tr>
<tr>
<td></td>
<td>2. How are experiments designed to assess whether they are successful?</td>
</tr>
<tr>
<td></td>
<td>3. How can business needs be addressed within architectural standards? When does a business need justify an exception to standard?</td>
</tr>
<tr>
<td>IT investment</td>
<td>1. What process changes or enhancements are strategically most important to the enterprise?</td>
</tr>
<tr>
<td></td>
<td>2. What are the distributions in the current and proposed IT portfolios? Are these portfolios consistent with the enterprise’s strategic objectives?</td>
</tr>
<tr>
<td></td>
<td>3. What is the relative importance of enterprise-wide versus business unit investments? Do actual investment practices reflect their relative importance?</td>
</tr>
</tbody>
</table>

The Investment Approval Process

While the overall Governance Arrangements Matrix addresses the two first IT governance questions: “What decisions must be made and who should make them?” the third governance question: “How will these decisions be made and monitored?” is tackled through the investment approval process.\textsuperscript{23}

The investment decision is often the most visible and controversial of the five key IT decisions. Some projects are approved, others are bounced, and the rest enter the organisational equivalent of suspended animation with the dreaded request from the decision makers to “redo the business case” or “provide more information.” Enterprises that get superior value from IT focus their investments on their strategic priorities, cognizant of the distinction between “must have” and “nice to have” IT capabilities.\textsuperscript{24}

\textsuperscript{22} Ibid., pp54-55.
\textsuperscript{23} Ibid., pp54-55.
\textsuperscript{24} Ibid., p45.
The investment decisions address three dilemmas:  
- How much to spend,
- What to spend it on, and
- How to reconcile the needs of different constituencies.

The IT investment process must determine how much to spend on IT. Given uncertain returns on IT spending, many executives wonder whether they are spending too much – or perhaps too little. They often look to industry benchmarks as a way of determining appropriate spending level. But in the successful companies studied by the Massachusetts Institute of Technology’s Sloan School of Management, benchmarks are only a starting point. Senior managers focus on the strategic role that IT plays in the organisation and establish an enterprise-wide funding level that will enable technology to fulfil its objective.  

The downsizing and reengineering initiatives so prevalent in recessive market situations have largely proved financially shortsighted. With hindsight, we now know that almost half of downsizing companies reported lower profits the year following their cutbacks. Despite the failure of across-the-board cost cutting, effective cost management is a critical discipline practiced by successful, value-creating companies.  

When looking at what to spend many enterprises find it useful to think of an enterprise’s IT investments as a portfolio. Portfolio management enables decision makers to align their portfolios with enterprise strategy and balance risk and returns. The IT portfolio concept assists managers in balancing and realigning their investments when the enterprise’s strategy or the economic climate changes. Comparisons of portfolios with industry benchmarks facilitate a discussion on how well aligned an IT portfolio is with the strategy and allow managers to make more informed investment decisions relative to the competition. A powerful question to ask is: Can we explain differences between our IT investment portfolio and the industry benchmark by our strategy? If the explanation is credible, the portfolio is a good fit. If the explanation is unconvincing, the IT investment process is failing.  

The professional services firm Gartner supports this method. To view IT holdings through the lens of portfolio analysis will reveal that each application category has a different set of decision makers, expected return on investment and level of acceptable risk. Even infrastructure systems, like security and telecommunications, can deliver business value, because they have the capability to significantly reduce business risk and enable new work styles.  

Investment processes must reconcile different needs, i.e. the demands of individual business units as well as demands to meet enterprise-wide needs. Enterprises that attempt to persuade independent business units to fund shared infrastructure are likely to experience resistance. Instead, business leaders must articulate the enterprise-wide objectives of shared

---

25 Ibid., p45.
26 Ibid., p45.
infrastructure and provide appropriate incentives for business unit leaders to sacrifice business unit needs in favour of enterprise-wide needs.  

The business value of IT is spread across a myriad of business processes and activities, yet the cumulative and ongoing annual costs of all these IT investments are quite apparent, especially if they are concentrated in one budget. It is tempting to view IT as just another cost centre; however, the business value of IT lies in its ability to conduct business processes more reliably, faster and at lower cost; and to control inventories, increase revenues, reduce time to market and provide information that enables better decisions. Therefore, assessing the business value means establishing a link between the investment and its contribution to business processes.

All businesses knowingly take risks that lead toward reward. The concept of cost benefit analyses of information security helps management make decisions on which initiatives to fund with how much, as there needs to be an approach for measuring and comparing different alternatives and how they meet business objectives of the enterprise. In a company that relies heavily on information, risks to that information tend mostly to be without reward. It is the job of security advisors to remove risk that is non-contributory to reward. Any company’s balance sheet has a finite tolerance for risk; security advisors contribute to business success by “purifying” the overall risk the company holds, allocating more of the available risk tolerance to risks that actually could bear fruit by removing the risks that, at best, lead nowhere. But to do this, the return on investment of security interventions must be measured.

Most enterprises formalise their IT investment proposal process to ensure that creative ideas and strategic priorities are considered by investment decision makers. Many enterprises use standardised IT investment approval application templates to estimate metrics such as return on investment, net present value, and risk for each project. Without investment templates, decision makers struggle to compare projects and can miss opportunities for value from investments with less certain benefits.

While standardised project proposals expose relative benefits and risks of individual projects, they are less effective in establishing how a proposed project contributes to an enterprise’s strategic objectives. Most enterprises rely on business units and functions to establish their priorities based on business unit and functions objectives. Investment committees typically determine the set of projects that together provide the greatest strategic benefits to the enterprise.

Non-financial Performance Metrics

Security decision-making tends naturally toward cost benefit analysis, a species of quantitative assessment that ultimately compares costs to benefits and rationally picks the greatest return. But this analysis has a flaw that can easily prove fatal: Costs and benefits must be quantified in the same currency. While this is easy when considering revenue-generating

---

30 Weill, Peter and Jeanne W. Ross, 2004, p49.
31 Roberts, John, 2002, p2
32 Geer, Daniel E. Jr., 2001, p1
34 Ibid., p98.
investments — money-in versus money-out — in the security world this is hard because, although money goes in, what comes back is hard to express in financial values. Examples include how to quantify reputation capital and the cost if customer doubt erases an enterprise’s first mover advantage. Cost benefit analysis, because it demands a common currency, is forever and always at risk of slipping an infinite numerator or a zero denominator into those ratios.

Governance Effectiveness

Understanding non-financial IT governance performance related to the specific enterprise is a fundamental part to be able to perform useful cost benefit analyses of proposed information security investments. According to the Massachusetts Institute of Technology’s Sloan School of Management the effectiveness of IT governance could be assessed in how well it meets four objectives:

1. Cost-effective use of IT
2. Effective use of IT for asset utilisation
3. Effective use of IT for growth
4. Effective use of IT for business flexibility

Market situations differ, as do enterprises’ strategies over time. By identifying the relative importance of the four different factors to the enterprise, the information security professional is able to understand what aspects need to be supported by an investment. The approach is based on asking the senior management team – the Institute recommends at least ten managers – to answer the following questions:

1. How important are the following outcomes of your IT governance, on a scale from 1 (not important) to 5 (very important)?
   - Cost-effective use of IT
   - Effective use of IT for asset utilisation
   - Effective use of IT for growth
   - Effective use of IT for business flexibility

2. What is the influence of the IT governance in your business on the following measures of success, on a scale from 1 (not successful) to 5 (very successful)?
   - Cost-effective use of IT
   - Effective use of IT for business flexibility
   - Effective use of IT for asset utilisation
   - Effective use of IT for growth

Effectiveness of IT Governance

Then average the results and look at variation by business units and level of management. Since not all firms rank the outcomes with the same importance, the answers to the first question is used to weight the answers to the second question. The weighted scores for the four questions are added and divided by the maximum score attainable by that enterprise. Therefore, mathematically, governance performance =

\[
\frac{\sum_{n=1}^{4} (\text{importance of IT governance outcome}\cdot\text{Q1}) \cdot \text{Influence of IT Governance}\cdot\text{Q2}) \cdot 100}{\sum_{n=1}^{4} (5 \cdot \text{importance of IT governance outcome})}
\]

Given that there are four objectives, the maximum score for any enterprise is 100 and the minimum score is 20.

---

35 Geer, Daniel E. Jr., 2001, p2
36 Weill, Peter and Jeanne W. Ross, 2004, p121.
37 Ibid., p121.
38 Ibid., pp239-240.
39 Ibid., pp239-240.
Risk Analysis

ITGI states that a key goal of information security is to reduce adverse impacts on the organisation to an acceptable level of risk. Therefore, an effective security programme will show a trend of impact reduction and quantitative measures can include trend analysis of impacts over time as an alternative to the factors described above. However, the fundamental purpose of internal control measures is to prevent or detect security breaches. If the solution prevents most incidents before they materialise, it could be deemed superfluous by management unless it is made transparent that the specific investment made an impact. On the other hand, if the implemented solution detect numerous of incidents that were not previously identified, there is a risk that stakeholders see this as a sign of ineffective information security governance, believing the number of incidents have risen.

Risk analysis is the most complex method of estimating profits. Due to the uncertainties involved in risk measurement and the concept of benefits being based on lowered “value-at-risk”, the risks are often assessed in abstract, or proprietary, terms, e.g. “High, Medium, Low” or 1-10. These estimates are then presented in heat maps, as shown below. Evaluating risks in this manner enables participants the opportunity to have a focused discussion, share opinions, review facts and arrive at a clearer definition and understanding of the risks – shared by all.

The risk assessment process is a method of determining what kind of controls are needed to protect an organisation’s information systems and other assets and resources not just adequately, but cost-effective. The terms risk analysis, risk assessment, business impact analysis (BIA), and threat- or vulnerability assessment are all used in this context. Basically, the risk analysis identifies risks, recommends steps to mitigate the risks, analyses the costs associated with that mitigation and correlates this information to determine feasibility.

---

40 Information Technology Governance Institute, 2003, p29
41 Kotler, Philip, and Kevin Lane Keller, 2006, p651
43 Raytheon Company, 2002.,p2
According to The University of Regensburg the risk analysis is useful for giving appropriate data input to the effectiveness measurement of information security management. The risk analysis is performed best as 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 IT 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 capital charge and the expected losses. 

Business Case Analysis
A common approach used for strategic investment decisions is the business case analysis (BCA). The professional services firm McKinsey & Company argue that this often involves underestimating uncertainty in order to lay out a vision of future events sufficiently precise to be captured in a financial analysis. Another danger lies at the other extreme: if managers can’t find a strategy that works under traditional analysis, they may abandon the analytical rigor of their planning process altogether and base their decisions on gut instinct.

Making systematically sound strategic decisions under uncertainty requires an approach that avoids dangerous binary views. Rarely do managers know absolutely nothing of strategic importance, even in the most uncertain environments. Available strategically relevant information tends to fall into two categories. First, it is often possible to identify clear trends, such as market demographics or risk exposure. Second, if the right analyses are performed, many factors that are currently unknown to an enterprise’s management are in fact knowable – for instance, performance attributes for current technologies, the elasticity of demand for certain stable categories of products, and competitors’ plans to expand capacity.

The uncertainty that remains after the best possible analysis has been undertaken is called residual uncertainty – e.g., the outcome of an ongoing regulatory debate or the performance attributes of a technology still in development. But quite a bit can often be known despite this. In practice the residual uncertainty facing most decision makers falls into one of four broad levels:

1. A clear enough future
2. Alternative futures
3. A range of futures
4. True ambiguity

At level one the residual uncertainty is irrelevant to making strategic decisions, so managers can develop a single forecast that is a sufficiently precise basis for their strategies. To help generate this usefully precise prediction of the future, managers can use the standard strategy tool kit: market research, analyses of competitors’ costs and capacity, value chain analysis, Michael Porter’s five-forces framework, and so on.

When the uncertainty is at level two the future can be described as one of a few discrete scenarios. Analysis can’t identify which outcome will actually come to pass, though it may

---

44 Locher, Christian, 2005, p9
45 Cortney, Hugh G., Jane Kirkland and S. Patrick Viguerie, 2001, pp5-6
46 Grant, Robert M., 2005, p319
47 Cortney, Hugh G., Jane Kirkland and S. Patrick Viguerie, 2001, pp6-9
48 Ibid., p6
help establish probabilities. Most important, some, if not all, elements of the investment would change if the outcome were predictable. Here, managers must develop a set of discrete scenarios based on their understanding of how the key residual uncertainties might play out. Each scenario may require a different valuation model. Getting information that helps establish the relative probabilities of the alternative outcomes should be a high priority. After establishing an appropriate valuation model for – and determining the probability of – each possible outcome, the risks and returns of alternative strategies can be evaluated with a classic decision analysis framework. Particular attention should be paid to the likely paths the industry might take to reach the alternative futures, so that the company can determine which possible trigger points to monitor closely. 49

A range of potential futures can be identified at level three. A limited number of key variables define that range, but the actual outcome may lie anywhere within it. There are no natural discrete scenarios. As in level two, some, and possibly all, elements of the strategy would change if the outcome were predictable. The analysis in level three is similar to that in level two. Developing a meaningful set of scenarios, however, is less straightforward in level three, but there are a few general rules. First, develop only a limited number of alternative scenarios-the complexity of juggling more than four or five tends to hinder decision-making. Second, avoid developing redundant scenarios that have no unique implications for strategic decision-making. Third, develop a set of scenarios that collectively account for the probable range of future outcomes and not necessarily the entire possible range. Establishing the range of scenarios should allow managers to decide how robust their strategies are, to identify likely winners and losers, and to determine, at least roughly, the risk of following status quo strategies. 50

At level four a number of dimensions of uncertainty interact to create an environment that is virtually impossible to predict. In contrast to level three situations, it is impossible to identify a range of potential outcomes, let alone scenarios within a range. It might not even be possible to identify, much less predict, all the relevant variables that will define the future. Level four situations are quite rare, and they tend to migrate toward one of the others over time, but they do exist. 51

Irrespective of the residual risk, a financial metrics model that incorporates the predictions of the scenario (or scenarios) should be used to determine the value of alternative strategies. 52

**Game Theory**

The theory of games is a set of methods, mostly worked out in the last century by a mathematician named John Von Neumann, and later embellished by others. Game theory is another way of evaluating the paths through a particular tree, or set of trees. It assumes that we have a contest between two or more players, each of which has something to win or lose. By setting up a matrix of possibilities, we can find out what chance one has of winning the contest, or at least maximizing the benefits. 53

---

49 Ibid., pp6-7  
50 Ibid., pp7-8  
51 Ibid., pp8-9  
52 Ibid., p6  
The University of Texas’ School of Management suggests game theoretical considerations as an alternative to the traditional risk- or business case scenarios. The data input for the game theory is based on risk (and behaviour) analysis and business considerations. They argue that information security has to do with the behaviour of attackers and defenders. Thus, approaches need to be used, which take into account the goals of the involved parties. Game theory enhances traditional decision theory by considering possible behaviour patterns of both parties (attackers and defenders). The decision resulting in an optimum of benefit is the best investment. In general, it can be criticised that the method always implies an intentional attacker. However, this approach may help security managers to plan security investments in a limited scope of application.  

Financial Performance Metrics

Irrespectively if the management of an enterprise uses risk analysis, IT governance performance metrics, business case scenarios, or any of the other approaches described above, they all ultimately seek to identify relevant financial business performance metrics. In order to set those financial metrics we need to understand the dominant Value Discipline of an enterprise. The table below, presented by the Massachusetts Institute of Technology’s Sloan School of Management, could be used.  

<table>
<thead>
<tr>
<th>Operational excellence</th>
<th>Customer intimacy</th>
<th>Product leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• End-to-end supply chain optimization</td>
<td>• Customer service, marketplace management</td>
<td>• Product development, time to market and market communications</td>
</tr>
<tr>
<td>• Emphasis on efficiency and reliability</td>
<td>• Emphasis on flexibility and responsiveness</td>
<td>• Emphasis on constant innovation</td>
</tr>
<tr>
<td>Organization and skills</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Central authority, low level of empowerment</td>
<td>• Empowerment close to point of customer contact</td>
<td>• Ad hoc, organic, and cellular</td>
</tr>
<tr>
<td>• Critical skills at core of organization (e.g., process management)</td>
<td>• Critical skills at boundary of organization (e.g., customer service)</td>
<td>• Critical technical skills abound in loose-knit structures</td>
</tr>
<tr>
<td>Management systems for coordination (e.g., incentives and IT architectures)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Command and control, standard operating procedures</td>
<td>• Customer equity measures like lifetime value</td>
<td>• Rewarding individuals’ innovative capacity</td>
</tr>
<tr>
<td>• Quality management</td>
<td>• Satisfaction, share management</td>
<td>• Risk and exposure management</td>
</tr>
<tr>
<td>Information and information systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Integrated low-cost transaction systems</td>
<td>• Single view of customer databases</td>
<td>• Systems for collaboration</td>
</tr>
<tr>
<td>• The system is the process</td>
<td>• Tools to identify segments and new offerings</td>
<td>• Modeling and simulation tools</td>
</tr>
<tr>
<td>Larger increases in ROA</td>
<td>Lower margins</td>
<td>Higher market cap growth and smaller increases in ROI and ROA</td>
</tr>
</tbody>
</table>


Three Value Disciplines

According to the Institute, the three alternative financial performance models are most relevant for IT governance:

- Asset utilisation
- Profit
- Growth

---

54 Cavusoglu, H. et al., 2004, pp. 65-75.
56 Ibid., pp121,160.
Accordingly, if the main Value Discipline is customer intimacy, profit is the financial dimension to focus on. Organisations driven by operational excellence should focus on asset utilisation, while companies dependent on product leadership should set their financial metrics at identifying potential for growth.  

Although many stakeholders are important to the overall success of the enterprise, the old adage, “He who pays the fiddler calls the tune,” tells the real story – the stakeholders funding the investment are the most important. The enterprise’s management style and culture will also play a role in selecting effective justification techniques (e.g., a risk-taking approach will be almost impossible to justify in a risk-adverse culture). Corporate culture certainly does not change rapidly, but it may be influenced over time. Management must not assume that what works in one enterprise will be effective in another.

Return on Investment (ROI) is a straightforward financial tool that measures the economic return of a project or investment. It is also known as return on capital employed. It measures the effectiveness of the investment by calculating the number of times the net benefits (benefits minus costs) recover the original investment. ROI has become one of the most popular metrics used to understand, evaluate, and compare the value of different investment options.

There are several variations of the Return on Investment (ROI) equation, given the multiple interpretations and applications in different industries. This lack of consistency in the definition of ROI causes confusion when comparing the ROI values of several projects. Below are the most common variations of the ROI equation:

**Return on Investment (ROI)**

![ROI formula](image)

**Definition of Terms**

- **net benefits**: Benefits minus costs.
- **costs**: Initial and recurring (or ongoing) costs.
- **Time Period**: The standard ROI equation is usually calculated for the first year of the investment. A one-year time period has become an industry standard since companies seek to recover their investment on the first year of operations of the project. This rule of thumb may not be applicable across organizations but it can give a first estimate of the benefits of a project.

---

57 Ibid., pp121,160.
58 Gomolski, Barbara, Jeremy Grigg, 2002, p1
59 Perks, Robert, 2004, pp381-384
**Return on Invested Capital (ROIC)**

\[
\text{ROIC} = \frac{\text{NOPAT}}{\text{invested capital}} \times 100\% 
\]

Definition of Terms

- NOPAT: Net operating profit after taxes.
- invested capital: Initial and recurring (or ongoing) costs.

**Return on Investment - Using Net Present Value or Discounted Cash Flow**

\[
\text{ROI} = \frac{\text{NPV (net benefits)}}{\text{PV (costs)}} \times 100\% 
\]

This equation accounts for the time value of money or the interest derived from an investment with similar risk. The Present Value is discounted according to the cost of capital to the company or the rate at which the company could borrow money in the marketplace, given its risk level. \(^{61}\)

Definition of Terms

- NPV (net benefits): Present value of benefits minus present value of costs.
- PV (costs): Present value of costs.

**Net Present Value (NPV)**

The Net Present Value (NPV) of a project or investment is defined as the sum of the present values of the annual cash flows minus the initial investment. The annual cash flows are the Net Benefits (revenues minus costs) generated from the investment during its lifetime. These cash flows are discounted or adjusted by incorporating the uncertainty and time value of money. NPV is one of the most robust financial evaluation tools to estimate the value of an investment. \(^{62}\)

The calculation of NPV involves three simple yet nontrivial steps. The first step is to identify the size and timing of the expected future cash flows generated by the project or investment. The second step is to determine the discount rate or the estimated rate of return for the project. The third step is to calculate the NPV using the equations shown below: \(^{63}\)

\[
\text{NPV} = \text{initial investment} + \frac{\text{Cash flow Year 1}}{(1+r)^1} + \cdots + \frac{\text{Cash flow Year n}}{(1+r)^n} 
\]

Or,

---

\(^{61}\) Ibid.
\(^{62}\) Ibid.
\(^{63}\) Ibid.
Definition of Terms

- **initial investment**: This is the investment made at the beginning of the project. The value is usually negative, since most projects involve an initial cash outflow. The initial investment can include hardware, software licensing fees, and start-up costs.
- **Cash flow**: The net cash flow for each year of the project: Benefits minus Costs.
- **Rate of Return (r)**: The rate of return is calculated by looking at comparable investment alternatives having similar risks. The rate of return is often referred to as the discount, interest, hurdle rate, or company cost of capital. Companies frequently use a standard rate for the project, as they approximate the risk of the project to be on average the risk of the company as a whole.
- **Time (t)**: This is the number of years representing the lifetime of the project.

A company should invest in a project only if the NPV is greater than or equal to zero. If the NPV is less than zero, the project will not provide enough financial benefits to justify the investment, since there are alternative investments that will earn at least the rate of return of the investment. In theory, a company will select all the projects with a positive NPV. However, because of capital or budget constraints, companies usually employ a concept called NPV Indexes to prioritize projects having the highest value. The NPV Indexes are calculated by dividing each project’s NPV by its initial cash outlay. The higher the NPV Index, the greater the investment opportunity.

The NPV analysis is highly flexible and can be combined with other financial evaluation tools such as Scenario analyses. NPV and Scenario Analysis are combined by varying a predetermined set of assumptions to determine the overall impact on the NPV value of the project.

**Internal Rate of Return (IRR)**

The Internal Rate of Return (IRR) is defined as the discount rate that makes the project have a zero Net Present Value (NPV). IRR is an alternative method of evaluating investments without estimating the discount rate. IRR takes into account the time value of money by considering the cash flows over the lifetime of a project. The IRR and NPV concepts are related but they are not equivalent. Companies should invest in opportunities with rates of return higher than the interest rate paid on capital plus a premium for risk.

The IRR uses the NPV equation as its starting point:

\[
\text{NPV} = \text{initial investment} + \sum_{t=1}^{t=\text{end of project}} \frac{(\text{Cash Flows at Year } t)}{(1+\text{IRR})^t}
\]
Definition of Terms

- initial investment: The investment at the beginning of the project.
- Cash flow: Measure of the actual cash generated by a company or the amount of cash earned after paying all expenses and taxes.
- IRR: Internal Rate of Return.
- n: Last year of the lifetime of the project.

Calculating the IRR is done through a trial-and-error process that looks for the Discount Rate that yields an NPV equal to zero, typically accomplished by using the IRR function in a spreadsheet program.  

For example, the IRR for a particular project is 20%, and the cost of capital to the company is only 12%. The company can approve the project because the maximum value for the company to make money would be 8% more than the cost of capital. If the company had a cost of capital for this particular project of 21%, then there would be a negative NPV and the project would not be considered a profitable one. The IRR is therefore the maximum allowable discount rate that would yield value considering the cost of capital and risk of the project. For this reason, the IRR is sometimes referred to as a break-even rate of return. It is the rate at which the value of cash outflow equals the value of cash inflow.

There are some special situations where the IRR concept can be misinterpreted. This is usually the case when periods of negative cash flow affect the value of IRR without accurately reflecting the underlying performance of the investment. Managers may misinterpret the IRR as the annual equivalent return on a given investment. This is not the case, as the IRR is the breakeven rate and does not provide an absolute view on the project return.

**Modified Internal Rate of Return (MIRR)**

While the internal rate of return (IRR) assumes the cash flows from a project are reinvested at the IRR, the modified IRR assumes that all cash flows are reinvested at the firm’s cost of capital. Therefore, MIRR more accurately reflects the profitability of a project.

For example, say a two-year project will cost USD 195 with a cost of capital of 12% and that it will return USD 110 in the first year and $121 in the second year. To find the IRR of the project so that the net present value (NPV) = 0:  

\[
NPV = 0 = -195 + 110/(1+ IRR) + 121/(1 + IRR)^2  
\]

NPV = 5 when IRR = 10%

Solving for NPV using MIRR, we will replace the IRR with our MIRR = cost of capital of 12%:

\[
NPV = -195 + 110/(1+ .12) + 121/(1 + .12)^2  
\]

NPV = -0.32 when MIRR = 12%

67 Ibid.
68 Ibid.
69 Ibid.
71 Ibid.
Thus, using the IRR could result in a positive NPV (good project), but it could turn out to be a bad project (NPV is negative) if the MIRR were used. As a result, using MIRR versus IRR better reflects the value of a project. 72

**Free Cash Flow (FCF)**

Free cash flow (FCF) represents the cash that a company is able to generate after laying out the money required to maintain/expand the company’s asset base. Free cash flow is important because it allows a company to pursue opportunities that enhance shareholder value. Without cash, it’s tough to pursue new opportunities, make acquisitions, pay dividends, and reduce debt, etc. 73

Some believe that analysts focus on short-sightedly earnings while ignoring the “real” cash that a firm generates. Accounting gimmicks can cloud earnings, but it’s tougher to fake cash flow. For this reason, some investors believe that FCF gives a much clearer view of the ability to generate cash (and thus profits). 74

It is important to note that negative free cash flow is not bad in itself. If free cash flow is negative, it could be a sign that a company is making large investments. If these investments earn a high return, the strategy has the potential to pay off in the long run. 75

**Discounted Cash Flow (DCF)**

The Discounted Cash Flow is a valuation method used to estimate the attractiveness of an investment opportunity. DCF analysis uses future free cash flow projections and discounts them to arrive at a present value, which is used to evaluate the potential for investment. Most often discounted by the weighted average cost of capital. If the value arrived at through DCF analysis is lower then the current cost of the investment, the opportunity may be a good one. 76

The basic formula is calculated as:

\[ DCF = \frac{CF_1}{(1+r)^1} + \frac{CF_2}{(1+r)^2} + \ldots + \frac{CF_n}{(1+r)^n} \]

**Definition of Terms**

- CF: Cash flow
- r: discounted rate (weighted average cost of capital)

DCF models are powerful but they do have shortcomings. DCF is merely a mechanical valuation tool, which makes it subject to the CICO principle (crap in-crap out). Small changes in inputs can result in large changes in the value of an investment. Instead of trying to project the cash flows to infinity, a terminal value approach is taken in the valuation. A simple
annuity is used to estimate the terminal value past three to five years for example. This is done because as time goes on, it is harder to come to a realistic estimate of the cash flows.  

**Payback Period**

The easiest way to deal with the timing of future returns is to as the simple question: how quickly do we get our money back? It is calculated as:  

\[
\text{Payback Period} = \frac{\text{Cost of Project}}{\text{Annual Cash Inflows}}
\]

With all other things being equal, the better investment is the one with the shorter payback period. There are two main problems with the payback period method:  

1. It ignores any benefits that occur after the payback period, and so does not measure profitability  
2. It ignores the time value of money

Because of these two reasons, other methods of capital budgeting like NPV, IRR, or DCF are generally preferred.

**Total Cost of Ownership (TCO)**

Total Cost of Ownership (TCO) can be defined as the systematic quantification of all costs generated over the lifetime of a project. The goal of TCO is to determine a figure that reflects the total cost of the investment, including one-time purchases and recurring costs, not just the initial start-up cost.

The TCO concept is widely used in Information Technology (IT) implementations where the benefits are hard to quantify and the focus is on minimizing the project costs. Companies use the TCO methodology when comparing similar products from different vendors. The product features among vendors may not be much different but the quality and support of the products may yield considerably different TCO values. Because benefits are not considered in TCO, the overall financial analysis is simplified. TCO may yield the wrong conclusions if the goal is not to minimize costs but to maximize the benefits with the smallest number of resources.

The Total Cost of Ownership (TCO) equation is the sum of all project costs including one-time as well as recurring costs. All these costs are determined by looking at each stage of a project, starting with planning, design, and installation, and moving through integration, training, and ongoing support and maintenance. Once all the costs have been identified and compiled, they are added up and divided by the project duration, calculated as:

\[
\text{TCO} = \frac{\sum_{t=1}^{t=\text{end of project}} \text{one time costs} + \text{recurring costs} (t)}{\text{project duration}}
\]

---

77 Ibid.  
78 Perks, Robert. 2004, pp384-386  
80 Ibid.  
82 Ibid.  
83 Ibid.
Definition of Terms

- **one time costs**: These are the costs that are derived at one stage during the implementation or operation of a project. One-time costs could include personnel training, new processes being introduced that yield one-time cost, or investment in infrastructure assets.

- **recurring costs**: These are costs that continue over time or repeat, e.g., continuous monitoring of performance.

- **project duration**: This is the project lifespan or a standard duration that is used to normalize all the TCO calculations across an enterprise.

**Total Benefit of Ownership (TBO)**

The TBO equation is not a new or revolutionary concept, but in recent years it has been expanded to include all the benefits of a project. The idea is to emphasize that the benefits of an implementation may be greater if other hidden benefits are included, such as customer satisfaction and product up-sells (persuading customers to buy more expensive items than they originally intended to buy or enabling new business channels).

The TBO equation is exactly the same as the TCO equation, but the benefits of the project are calculated rather than the costs.

\[
TBO = \sum_{t=1}^{t=\text{end of project}} \frac{\text{one time benefits} + \text{recurring benefits} (t)}{\text{project duration}}
\]

Definition of Terms

- **one time benefits**: These are the benefits that are derived at one stage during the implementation or operation of a project. For example, one-time benefits could include personnel reductions, process changes that yield one-time payoffs, or consolidation of assets.

- **recurring benefits**: These are benefits that continue over time or repeat, such as improvements in productivity or performance, or increases in customer satisfaction.

- **project duration**: This is the project lifespan or a standard duration that is used to normalize all the TBO calculations across an enterprise.

**Economic Value Add (EVA)**

In the field of corporate finance, working capital management is useful to improve a firm’s financial performance metrics. Economic value added is a way to determine the value created, above the required return, for the shareholders of a company.

The basic formula is calculated as:

\[
EVA = (r - c) \cdot K = NOPAT - c \cdot K
\]

---

84 Ibid.
85 Ibid.
Definition of Terms

- $r$: The return on capital employed (ROCE) defined as $r = \frac{\text{NOPAT}}{K}$
- NOPAT: The Net Operating Profit After Tax
- $c$: The Weighted Average Cost of Capital (WACC)
- $K$: capital employed.

Shareholders of the company will receive a positive value added when the return from the equity employed in the business operations is greater than the cost of that capital. Any value obtained by employees of the company or by product users is not included in the calculations.

**Return On Security Investment (ROSI)**

Financial performance measures do not consider security-specific data (e.g. threats, vulnerability, risk) as a decision variable. As a vehicle, security managers – striving to find variables to judge the need for a particular investment – have developed models in the field of security economics. The effects are the consideration of risk effects and the ability to integrate in common accounting concepts.  

The Return On Security Investments (ROSI) formula, developed by a team at the University of Idaho led by researcher HuaQiang Wei, is the most well known ROSI calculation in the security industry. They used what they found in the research area of information security investments and combined it with some of their own theories, assigning values to everything from tangible assets (measured in dollars with depreciation taken into account) to intangible assets (measured in relative value, for example, software A is three times as valuable as software B). Different types of attacks, or incidents, were assigned individual costs. To verify the model, the team went about attacking an intrusion detection box they had built, to see if the costs the simulation produced matched the theoretical costs. They did. Determining cost-benefit became the simple task of subtracting the security investment from the damage prevented.

The risk mitigation effects show the benefit of a security investment: it is basically a “savings” in Value-at-Risk; it comes by reducing the risk associated with losing some financial value.

It is calculated as:

\[
\text{ROSI} = R - (R - E) + T, \\
\text{or} \\
\text{ROSI} = R - \text{ALE}, \text{ where } \text{ALE} = (R - E) + T
\]

**Definition of Terms**

- ALE: What we expect to lose in a year (Annual Loss Expectancy)
- $R$: The cost per year to recover from any number of incidents.
- $E$: These are the financial annual savings gained by mitigating any number of incidents through the introduction of the security solution.
- $T$: The annual cost of the security investment.

---

86 Locher, Christian, 2005, p9
87 Berinato, Scott, 2002, p5
A security investment is judged to be profitable, if the risk mitigation effect is greater than the expected costs. The formula helps for decisions about one investment, not setting priorities in more alternatives, because it lacks the relation to the capital employed. As a result, the marginal cost of security is in the hand of the decision maker.  

The impracticality of ALE-based methodologies, with their massive assessment needs, has forced risk managers to develop alternatives that would be less prone to controversy and more easily implemented. Recalling that risk is made up of consequences and their respective likelihoods, or frequencies, of occurrence and that no sufficiently detailed statistics are available to predict those likelihoods, Kevin J. Soo Hoo of Stanford University suggests that a reasonable simplification might be to ignore the likelihood half of the risk definition.  

Others, e.g., Christian Locher, at the University of Regensburg, suggest a more detailed definition of loss and loss effects compared to the Idaho method. They claim it would lead to more relevant results if the risk mitigation effects were calculated properly with scenario analysis and expected values.

---

89 Locher, Christian, 2005, p8
90 Soo Hoo, Kevin J, 2000, p9
EMPIRICAL DATA

Enterprises have struggled to understand the value of their IT-related initiatives because value cannot always be readily demonstrated through a traditional discounted cash flow analysis. Value results not only from incremental process improvements but also from the ability to respond to competitive pressure. In the past years managing the value network has required enterprises to make increasing investments in major enterprise resource planning (ERP) systems to manage cash-flow, manufacturing, human resources, purchasing and other major functions within a unified framework. There have been spectacular failures of large IT investments – initiatives that were never completed, e-business initiatives that were ill-conceived or poorly executed, and data mining experiments that generated plenty of data but few valuable leads.

As IT implementations enable increasing standardisation and integration of business processes, the roles of technologists and business leaders become increasingly intertwined. IT decision-making necessarily becomes joint decision-making. Successful firms not only make better IT decisions, they also have better IT decision-making processes. Specifically, successful firms involve the right people in the process.

**Governance Arrangements**

According to research performed by The Massachusetts Institute of Technology’s Sloan School of Management, three approaches dominate IT investment and prioritisation decision-making – business monarchies, federal and duopolies. The three approaches are almost equally popular, but they offer different views of how enterprises ensure maximum value from IT investments. That only nine percent of enterprises place IT investment decisions in the hands of IT professionals reflects the growing awareness that IT investments decisions involve business tradeoffs – decision makers determine which business processes will and will not receive IT support.

This is confirmed by one of the world’s largest and longest running annual surveys, performed by the professional services firm Ernst & Young. 42 percent of nearly 1,200 respondents report that it is the Chief Information Officer (CIO) that owns the information security process, while the second most common decision maker is the Chief Executive Officer (CEO), with 17 percent. The same two stakeholders are most commonly approving the information security budgets. In 31 percent of the cases it is the CEO, while 26 percent of the respondents rely on their CIO to make the approvals.

Business monarchies are well positioned to define and fund business priorities. Business monarchies are typically also responsible for overall capital budgeting decisions. Thus, vesting responsibility for IT or information security investment and prioritisation in a business monarchy allows projects to compete for funds with other organisational needs. The

---

92 Kotler, Philip, and Kevin Lane Keller, 2006, pp470-472
94 Ibid., p16.
95 Ibid., pp69-70.
96 Ernst & Young, 2006. Accessed 2007-06-17
competition for funding facilitates an integrated view on the enterprise’s key assets and is aided by an enterprise investment committee that looks at all major investments. 97

Federal approaches to IT investment balance enterprise-wide priorities with business unit priorities. The relative balance of the federation strength varies between companies. Some let a majority of the funding be allocated by the senior management team, with the business units being given “allowance” for business unit priorities. Other firms have highly autonomous business units fund most IT from their regional offices, using occasional central funding to address strategic global needs. 98

Duopoly approaches (often T-shaped committees) to IT investment recognise that the IT unit is uniquely positioned to identify the risks posed by the existing IT infrastructure and the opportunities for sharing and reuse across business units. Thus, the involvement of IT in the investment decision provides a longer-term view of the implications of currently funded projects. Senior executives can simultaneously ensure that priority projects are “staged” according to the need for and availability of needed infrastructure. Enterprises with strong duopolies can group projects requiring new infrastructure capabilities. This process allows faster payback on infrastructure because major infrastructure investments are delayed until a critical mass justifies the investment. 99

Data from Ernst & Young show that corporate leaders are starting to recognize that information security needs to have a permanent place at the risk management table to help with compliance, as well as proactively identify and manage other enterprise-wide risk areas. Nearly two thirds of survey respondents say their companies use regular meetings, steering groups, and formal frameworks to ensure information security involvement. A growing percentage of survey participants – 43 percent in 2006, compared with 40 percent in 2005 – say information security is integrated with their organizations’ risk management programs and processes. 100

When the Massachusetts Institute of Technology’s Sloan School of Management measured the effectiveness of IT governance in 256 enterprises, they found the average score to be 69. The top one third of enterprises scored over 74. Given that there were four objectives, the maximum score for all enterprises was 100 and the minimum score 20. 101 In the same study, the Institute used the Governance Arrangements Matrix to understand how companies governed their IT decisions. They concluded the following results: 102

97 Weill, Peter and Jeanne W. Ross, 2004, p70.
98 Ibid., p70.
99 Ibid., p70.
100 Ernst & Young, 2006. Accessed 2007-06-17
101 Weill, Peter and Jeanne W. Ross, 2004, p121.
102 Weill, Peter and Jeanne W. Ross, 2004 (II), p8
One area specifically identified as challenging for the 256 respondents was the investment approval process. The desirable behaviour was to have different investment approaches for different investment types and to consider IT as any another business investment, while there was an identified risk for undesirable behaviour in the form of breaking up the IT investments in smaller projects to avoid formalistic requirements on cost benefit analysis.¹⁰³

**Case Study: Information Security Governance at Motorola**

Motorola is a world leader in wireless and broadband communications. Their corporate approach includes designing and delivering what they call “must have” products, “must do” experiences and powerful networks — along with a full complement of support services. The company operates in three business segments: Connected Home Solutions, Mobile Devices and Networks & Enterprise. Motorola is a Fortune 100 company with global presence and impact. In 2006 Motorola had sales of USD 42.9 billion, which is nearly double the sales the company had in 2002.¹⁰⁴

Motorola offers an example of a company pursuing growth while managing the inherent security issues. Motorola has rebounded from very difficult market conditions following the extraordinary telecom and dot-com boom in the late 1990s. In 2003 Motorola management believed the firm to be poised for growth as the global economy recovered. At that time growth for Motorola would result from leveraging strong customer relationships and continued innovation in software applications and products. In 2007 the company’s Chairman and CEO, Ed Zander, promotes the corporate vision of seamless mobility – building simple and seamless connections to people, information, and entertainment – and the opportunity it

---

¹⁰³ Weill, Peter and Jeanne W. Ross, 2004, pp145-146
brings to Motorola. The focus for 2007 is still on profitable growth, this time accompanied by selective pursuit of market share, and continuous investments for the future of Motorola.\textsuperscript{105}

Because the software and telecommunications industries are particularly vulnerable to security risks, Motorola management believes that information security is critical to its growth objectives. Management defines information security as protecting information and systems from failures of availability, confidentiality, and integrity. This commitment has made information security a senior management issue and an integral part of corporate governance at Motorola.\textsuperscript{106}

Motorola has committed to information security in both operations and its products. Even with a clear growth strategy driving the enterprise, Motorola in 2006 undertook a cost-reduction action to reduce the number of facilities, including manufacturing facilities. Management is aware that despite specific business continuity and risk management plans are in place, the reduced number of alternative facilities could cause the period of any manufacturing disruptions to be longer. As a result, Motorola could have difficulties fulfilling their orders and sales with profits declining as a result.\textsuperscript{107}

IT governance at Motorola relies on close IT-business relationships at both the corporate and sector level (business segments). The CIO is on the executive team and participates in decisions on principles and investment with the Management Board. At the time of the study, the CIO’s leadership team consisted of the heads of architecture, infrastructure, enterprise applications, and security and the CIOs of the sectors. The CIO’s leadership team is responsible for both architecture and infrastructure decisions. Business application decisions involve negotiations between corporate leaders, sector IT leaders, and business unit heads in a duopoly arrangement.\textsuperscript{108}

\begin{flushright}
\textsuperscript{105} Motorola, Inc., 2006. Accessed 2007-06-17
\textsuperscript{106} Motorola, Inc., 2007 (II). Accessed 2007-06-17
\textsuperscript{108} Weill, Peter and Jeanne W. Ross, 2004, pp78-79.
\end{flushright}
Information Security Governance at Motorola

Motorola’s Chief Information Security Officer (CISO) who reports to the CIO, joins the CIO at quarterly Management Board meetings. In these meetings, the security officer details Motorola’s security risks and alternatives for addressing them. A key element of information security governance is ongoing education. The security officer has worked with senior management on how to think about the likelihood of various security breaches and the potential impacts of each threat on the business.  

As with other areas of IT governance, the Management Board establishes security principles and defines priorities. The Board specifies the security budget separately from the rest of the IT budget. Motorola implements its security plans at both corporate and sector level. The CISO’s staff designs and builds appropriate technology. Security staff members also work with IT architects at both the corporate and the sector levels to ensure that security measures are seamlessly built into infrastructure and applications.  

The security-based governance initiatives at Motorola provide an example of how enterprises govern to address strategic issues. Motorola’s security concerns are reflected in its organisational structure and roles, governance arrangements, and specific architecture.

---

109 Ibid., pp79-80.
110 Ibid., p80.
processes. Many enterprises are concerned with security, but Motorola has made it a strategic priority. Its governance arrangements ensure that information security considerations are built into desirable behaviour.  

Case Study: Cost Benefit Analysis of Security Investment at Ericsson

Ericsson is a world-leading provider of telecommunications equipment and related services to mobile and fixed network operators globally. Over 1,000 networks in 140 countries utilize network equipment from Ericsson and 40 percent of all mobile calls are made through systems developed by the company. Ericsson is one of the few companies worldwide that can offer end-to-end solutions for all major mobile communication standards. Ericsson invests heavily in research and development (R&D) and actively promotes open standards and systems. Also reflecting its ongoing commitment to technological leadership, it has one of the industry’s most comprehensive intellectual property portfolio containing over 20,000 patents.

Ericsson is managed through common processes, where risk management is integrated, applying various methods for risk assessment and control, to ensure that the risks the company is exposed to are managed according to established policies. The parent company is Telefonaktiebolaget LM Ericsson, and group functions reside within that company. Ericsson’s Chief Information Security Officer (CISO) is a member of the group function Corporate Security, headed by the Chief Security Officer (CSO). The group functions formulate group strategy, issue policies and directives, perform business control, resource allocation and risk management.

In the early 2000’s, Ericsson went through a serious financial situation due to the market conditions. Having been a firm of more than 100,000 employees in the year 2000, the company found itself forced to cut back more than half of its staff during the period 2000-2004. In parallel all IS/IT was outsourced to external suppliers. During 2003 the enterprise was still driven by cost control measures balanced with retained information security governance, while optimising its IS/IT operations.

During the IT outsourcing program at Ericsson, the company kept a small number of business critical applications within the enterprise. Examples include the group consolidation system and its certification authority system. A certification authority based on Public Key Infrastructure (PKI) technology is part of the enterprise-wide infrastructure, and is used to create securely authenticated certificates. If properly implemented a PKI enables a company to communicate via encrypted channels, create legally accepted signed electronic transactions and records as well as ensuring accountability in logs and secure electronic payments. Ericsson and other multinational companies define the different types of certificates depending on their intended liability and use at the company. These levels are defined in the Certificate Value Statement (CVS).

---

111 Ibid., p80.
114 Ernst & Young, 2003.
115 Cardholm, Lucas, May-Lis Farnes and Andreas Halvarsson, 2001, pp10-12
PKI is driven by business requirements and should provide a positive return on investment – “the carrot”, but is also driven by legal/regulatory security requirements – “the stick”. Being part of the enterprise-wide infrastructure, it touches many business processes, crosses organizational boundaries and has a complex implementation cycle. When integrated into business processes, it provides a ROI through:

1. Lower operating costs;
2. Legal/regulatory compliance;
3. Improved service;
4. Extended reach;
5. A jump on the competition; and
6. Increased security.

The IT management of Ericsson had identified an opportunity to outsource the PKI, as this would fit the overall outsourcing program and the demand-supply processes being put in place. The group function Corporate Security, being the system owner at the parent company, performed a legal risk analysis to assess if there were any legal requirements that would prevent the system of being outsourced. The analysis comprised the laws and regulations of all major jurisdictions, relevant to Ericsson, regarding legally binding electronic signatures, use of encryption technology and the storage of electronic records. The conclusion was that there were no legal requirements prohibiting the system to be outsourced to an independent third party. From a business risk perspective, though, it was recommended not to outsource it to the same IT suppliers that managed other infrastructure components or business applications relying on the integrity of the PKI, as this would expose the system to risks of ineffective segregation of duties. It was also stated that the IT Management should perform a formal cost analysis.

The aim of the cost analysis was to present the fundament for a decision whether to keep the sensitive system as an internally operated system or to outsource it to an independent third party. To ensure a reasonable chance of covering the actual future outcome of certificate-use in the market, scenarios were developed. The first market scenario presented a relatively low market penetration grade, while the second scenario covered a relatively high penetration grade. It was reasonable to assume that the future use of certificates would be somewhere within the range of these two scenarios, therefore a third scenario was developed, with a market penetration between the first two.

The primary variable driven by market development was the number of certificates to be issued by the system. Potential users of these certificates were both staff at Ericsson and its corporate customers and partners, but also consumers acquiring SonyEricsson mobile phones with pre-installed certificates for mobile e-business. In order to estimate the possible number of certificates to be issued within a 5-year period, the different scenarios were developed. These were based on market research and the experience of the professional services firm conducting the analysis. Internal resources from Ericsson and SonyEricsson validated the market data and variables proposed.

---

118 Ernst & Young, 2003.  
119 Ibid.  
120 Ibid.
The three business case scenarios were individually documented in the form of an introductory text describing a plausible market situation in 2007, and how the market had developed since 2003 to reach that state. Factors taken into account were either external (e.g. the growth rate of the telecom industry, Ericsson’s future market share and the use of mobile e-business among consumers), or internal (e.g. the perseverance of Ericsson management in enforcing laptop encryption based on certificates and the number of pre-installed certificates in SonyEricsson handheld devices). For each scenario the same set of variables were defined and compared, e.g. the number of users and systems that could be expected to utilise different types of certificates (different types of certificates require different types of processes and infrastructure) and the expected life-span of these certificates (some vendors charged per issued certificate, while others charged per user irrespective of the number of certificates issued) etc. 121

Only figures for the current state (Jan 2003) and the projected final state (Dec 2007) were relevant, as the progress of certificate expansion was modelled with three different projections in parallel: exponential development, inverted exponential, and linear development. 122

![Relative development curves for lowest/highest penetration of certificates](image)

When the scenarios had been defined, populated and approved by relevant stakeholders, external suppliers gave their price indications in respect of the different scenarios presented, and specifications on e.g. hardware requirements. All price indications were calculated using a CBA Workbook developed by Ernst & Young, where different discount levels regarding the costs per user were applied together with price levels regarding fixed costs refined by different types of related costs. All price models were compared using the three different development curves, to assess what the total difference in cost would be for a specific vendor solution, or combination of vendors, depending on how the market would take off. Cost calculations were based on the cash-flow principle (due to NPV) and a 5-year period was applied with an Internal Rate set to a level decided by Ericsson. By applying calculations on the lowest and highest total costs of different suppliers (or a combination of suppliers) for each scenario, a comparable overview on relative costs were performed. 123

---

121 Ibid.
122 Ibid.
123 Ibid.
The final report presented financial findings per scenario in the form of highest/lowest TCO if the PKI was kept internally and if it was outsourced. The financial figures were presented only as relative to each other, with all redundant cost variables removed to clarify the financial differences. To avoid any influence except for the financial data, no vendors were named in the management summary comparison. The financial findings were however complemented by non-financial findings related to the potential decisions. Ericsson has not made these findings public. 124

The case from Ericsson demonstrate how an information security investment can be supported by performing a cost benefit analysis using both traditional marketing approaches of business case analysis (BCA) as well as traditional financial calculations, without involving the most commonly used formula: return on information security investment (ROSI).

124 Ibid.
ANALYSIS

Much has been written on the failure of information security mechanisms to protect end users from privacy violations and fraud. This misses the point. The real driving forces behind security system design usually have nothing to do with such altruistic goals. They are much more likely to be the desire to grab a monopoly, to charge different prices to different users for essentially the same service, and to dump risk. Often this is perfectly rational. As information security is about power and money – about raising barriers to trade, segmenting markets and differentiating products – the security professional should not feel restricted to technical tools like cryptanalysis and information flow.125

The Information Security Investment Process

The information security investment process includes the aspects of how much to spend, what to spend it on, and how to reconcile the needs of different stakeholders. But to be able to properly address these concerns, the investment process needs to be understood from a governance perspective:

- Who makes the investment decisions?
- How are investment decisions measured in terms of effective management?
- How will these decisions be captured and monitored in financial terms?

Information security investments should deliver value. These should be optimised to support organisational objectives. Security activities consume resources. Optimal investment levels occur when strategic goals for security are achieved and an acceptable risk posture is attained by the organisation at the lowest possible cost.

Consider the following approach to cover these aspects:

1. Understand main rationale for the security investment
2. Identify stakeholders and strategic goals
3. Perform Cost Benefit Analysis
4. Validate that the results are relevant to stakeholders and strategic goals

There are mainly three driving forces that create the main rationale for information security investments. The first is that someone (from within or outside the enterprise) identify risks or gaps in the current control environment that need to be addressed. The second is business-driven IT-investments that need security mechanisms to mitigate risks associated with the investment. The third, and less common, alternative is identified security investment opportunities that would increase profitability, improved asset utilisation or enable growth for the enterprise.

<table>
<thead>
<tr>
<th>Main Rationale</th>
<th>Key questions to address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate risk in current control environment</td>
<td>What business values are at stake?</td>
</tr>
<tr>
<td></td>
<td>Who decides which risk level should apply?</td>
</tr>
<tr>
<td>Business-driven investment require security measures</td>
<td>What are the targets for the business-driven investment</td>
</tr>
<tr>
<td>Opportunity for business improvement</td>
<td>What types of improvement effects are anticipated (asset utilisation, profitability or growth)?</td>
</tr>
</tbody>
</table>

125 Anderson, Ross, 2001, p8
When the main rational for a security investment is clarified, the security professional need to identify stakeholders and understand the strategic goals to ensure that the cost benefit analysis will be able to deliver valuable input to the investment decision. To identify decision makers the information security professional need to ensure a proper understanding of the governance model for the enterprise. The Governance Arrangements Matrix, presented by the Massachusetts Institute of Technology’s Sloan School of Management, can help identify what archetype of governance arrangements exist for the specific investment.

<table>
<thead>
<tr>
<th>#</th>
<th>Archetype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business Monarchy</td>
<td>Top management of the enterprise</td>
</tr>
<tr>
<td>2</td>
<td>IT Monarchy</td>
<td>IT specialists</td>
</tr>
<tr>
<td>3</td>
<td>Feudal</td>
<td>Each business unit makes independent choices</td>
</tr>
<tr>
<td>4</td>
<td>Federal</td>
<td>Combination of the group functions and the business units with or without IT involved</td>
</tr>
<tr>
<td>5</td>
<td>IT Duopoly</td>
<td>IT group and one other group (i.e. top management or business unit leaders)</td>
</tr>
<tr>
<td>6</td>
<td>Anarchy</td>
<td>Isolated individual or small group decision making</td>
</tr>
</tbody>
</table>

An enterprise is driven by the overall business plan. The business plan is broken down into strategic decisions, and key targets and strategic goals for management to meet. Depending on which stakeholders are involved in an investment decision, their different targets and goals will have different impact on the decision. The information security professional need to ensure a proper understanding of what key targets and strategic goals drive the decision makers in this specific case, and where the funding will come from. It is not always the same as the group of decision makers that assess the cost benefit analysis. Before the CBA is performed, the following questions should be considered:

- Who will make the formal investment decision?
- Who will fund the investment?
- What other stakeholders could have an impact on the decision?
- What are the key targets and strategic goals for these stakeholders?

The five basic objectives for information security governance, as defined by the IT Governance Institute, may provide guidance.

<table>
<thead>
<tr>
<th>Basic Objective</th>
<th>Illustrative goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Strategic</td>
<td>• Ensure transparency and understanding of IT security costs, benefits, strategies,</td>
</tr>
<tr>
<td>Alignment</td>
<td>policies and service levels.</td>
</tr>
<tr>
<td></td>
<td>• Develop a common and comprehensive set of IT security policies.</td>
</tr>
<tr>
<td></td>
<td>• Communicate the IT strategy, policies and control framework.</td>
</tr>
<tr>
<td></td>
<td>• Enforce IT security policies.</td>
</tr>
<tr>
<td></td>
<td>• Define security incidents in business impact terms.</td>
</tr>
<tr>
<td></td>
<td>• Establish clarity on the business impact of risks to IT objectives and resources.</td>
</tr>
<tr>
<td></td>
<td>• Establish IT continuity plan that supports business continuity plans.</td>
</tr>
<tr>
<td>2. Risk Management</td>
<td>• Account for and protect all IT assets.</td>
</tr>
<tr>
<td></td>
<td>• Establish and reduce the likelihood and impact of IT security risks.</td>
</tr>
<tr>
<td></td>
<td>• Perform regular risk assessments with senior managers and key staff.</td>
</tr>
<tr>
<td></td>
<td>• Permit access to critical and sensitive data only to authorised users.</td>
</tr>
<tr>
<td></td>
<td>• Ensure critical and confidential information is withheld from those who should not have access to it.</td>
</tr>
<tr>
<td></td>
<td>• Identify, monitor and report security vulnerabilities and incidents.</td>
</tr>
<tr>
<td></td>
<td>• Develop IT continuity plans that can be executed and are tested and maintained.</td>
</tr>
</tbody>
</table>
3. Resource Management

- Maintain the integrity of information and processing infrastructure.
- Account for and protect all IT assets.
- Ensure that IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.
- Ensure proper use and performance of the applications and technology solutions.

4. Performance Measurement

- Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Time to grant, change and remove access privileges
- Number and type of suspected and actual access violations
- Number and type of malicious code prevented
- Number and type of security incidents
- Number and type of obsolete accounts
- Number of unauthorised IP addresses, ports and traffic types denied
- Number of access rights authorised, revoked, reset or changed

5. Value Delivery

- Ensure automated business transactions and information exchanges can be trusted.
- Make sure that IT services are available as required.
- Minimise the probability of IT service interruption.
- Minimise the impact of security vulnerabilities and incidents.
- Ensure minimum business impact in the event of an IT service disruption or change.
- Establish cost-effective action plans for critical IT risks

The security professional need also to ensure that the formal performance factors of the investment are considered in the cost benefit analysis:

- What performance factors are formally evaluated in the investment decision

When these factors are identified and documented the \textit{cost benefit analysis can be performed}. The CBA needs to reflect the rationale, by identifying relevant performance metrics, both non-financial and financial. A cost benefit analysis with only non-financial data is not acceptable from an investment decision-making perspective. At the same time, an analysis with only financial data may very well be decided upon, but the enterprise could end up having stakeholders that underestimate the risks involved in the investment or do not fully comprehend intangible benefits of the suggested solution.

Non-financial Performance Metrics

The different types of non-financial metrics described in this thesis are shown in the table below.

<table>
<thead>
<tr>
<th>Performance metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance effectiveness</td>
<td>Defines how well the solution is aligned with the enterprise’s governance principles</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Defines risks, probabilities and potential business impact if realised</td>
</tr>
<tr>
<td>Business Case Analysis</td>
<td>Describes future state, or states, for the suggested solution and its environment</td>
</tr>
<tr>
<td>Game Theory</td>
<td>Defines alternative strategies for attackers and defenders of information</td>
</tr>
</tbody>
</table>

Governance Effectiveness

When analysing investments that improve the internal controls of the enterprise, the principles for effective governance defined by the Massachusetts Institute of Technology’s Sloan School of Management, could be applied. The expected effectiveness of the information security investment could then be assessed by how well it meets four objectives weighted by their importance to the enterprise.
The approach is based on asking the senior management team – the Institute recommends at least ten managers – to answer questions by giving them a score between 1 and 5 in the tables below. Then average the results and look at variation by business units and level of management to meet the stakeholder composition for the investment decision:

### Importance of information security investment
How important are the following outcomes of your information security governance, on a scale from 1 (not important) to 5 (very important)?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cost-effective use of information security</td>
</tr>
<tr>
<td></td>
<td>Effective use of information security for growth</td>
</tr>
<tr>
<td></td>
<td>Effective use of information security for asset utilisation</td>
</tr>
<tr>
<td></td>
<td>Effective use of information security for business flexibility</td>
</tr>
</tbody>
</table>

### Influence of information security investment
What is the anticipated influence of the proposed information security investment in your business on the following measures of success, on a scale from 1 (not successful) to 5 (very successful)?

<table>
<thead>
<tr>
<th>Importance</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cost-effective use of information security</td>
</tr>
<tr>
<td></td>
<td>Effective use of information security for growth</td>
</tr>
<tr>
<td></td>
<td>Effective use of information security for asset utilisation</td>
</tr>
<tr>
<td></td>
<td>Effective use of information security for business flexibility</td>
</tr>
</tbody>
</table>

The first question assesses the importance of a particular outcome related to information security governance and the second question assesses how well the proposed information security investment contributes to meeting that outcome. Since not all firms rank the outcomes with the same importance, the answers to the first question is used to weight the answers to the second question. Then the weighted scores for the four questions are added and divided by the maximum score attainable by that enterprise. Therefore, mathematically, information security governance performance =

\[ \frac{\sum_{n=1}^{4} \text{(importance of information security governance outcome) \times \text{Influence of proposed information security investment)}}{\sum_{n=1}^{4} \text{(importance of information security governance outcome)}} \times 100 \]

Given that there are four objectives, the maximum score for the investment is 100 and the minimum score is 20.

Depending on what main rationale is driving the potential investment in information security, the governance effectiveness metric may be more or less relevant to the cost benefit analysis.

<table>
<thead>
<tr>
<th>Main Rationale</th>
<th>Probable relevance to CBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate risk in current control environment</td>
<td>High</td>
</tr>
<tr>
<td>Business-driven investment require security measures</td>
<td>Low</td>
</tr>
<tr>
<td>Opportunity for business improvement</td>
<td>Medium</td>
</tr>
</tbody>
</table>

### Risk Analysis
An effective security programme will show a trend of impact reduction and quantitative measures can include trend analysis of impacts over time. Due to this, the risk analysis is the most common starting point for information security investments. In the case study of
Motorola we could see that that Motorola’s CISO joins the CIO at quarterly Management Board meetings. In these meetings, the security officer details Motorola’s security risks and alternatives for addressing them.

There are different types of risk analyses, e.g. the business impact analysis or the threat- and vulnerabilities assessment. The methodologies aim at identifying

- What risks exist
- The probability of the risks being realised
- The impact of the risks if they are realised

The subject to risk analysis is often the applications used by the business units because they are in the centre of contractual agreements between the IT department and the business units. 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 IT department support in quantifying 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 financial influence of the expected losses. Too often the risk analysis does not specify what specific key targets and strategic goals of the stakeholders could influenced and at what financial levels. There are no reasons not to include these in the analysis, e.g. weak controls in the revenue recognition process could lead to loss of revenues due to fraud.

At Ericsson, we could see that the investment process was started by performing a legal risk analysis, aimed at identifying legal risks connected with keeping an internal PKI or relying on an outsourced system. The business owner of the system performed the analysis.

If a risk analysis identify wilful misconduct, the use of game theory could be useful in order to prioritise the risks and their counter-measures.

The risk analysis approach is useful in many situations. It could be used to identify weaknesses in the current operations of processes or systems, as well as looking at business-driven investments and identify risks related to those investments. Depending on what main rationale is driving the potential investment in information security, the risk analysis metric may be more or less relevant to the cost benefit analysis.

<table>
<thead>
<tr>
<th>Main Rationale</th>
<th>Probable relevance to CBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate risk in current control environment</td>
<td>High</td>
</tr>
<tr>
<td>Business-driven investment require security measures</td>
<td>High</td>
</tr>
<tr>
<td>Opportunity for business improvement</td>
<td>High</td>
</tr>
</tbody>
</table>

**Business Case Analysis**

By nature, the business case analysis (BCA) is focused on identifying solutions to meet stakeholder key targets and strategic goals. Making systematically sound strategic decisions under uncertainty requires an approach that includes managing risks. Rarely do security professionals know absolutely nothing of strategic importance, even in the most uncertain environments. As pointed out by the professional services firm McKinsey & Company, it is often possible to identify clear trends, such as market demographics or common risk exposures. Many factors can often be identified, e.g. performance attributes for current technologies or benchmark data on similar investments ion the industry. Using these known factors still leave some residual uncertainty. The business case analysis, or scenario-based
approach, can be quite useful to assess security investments. In practice the residual uncertainty falls into one of four broad levels:

1. A clear enough future
2. Alternative futures
3. A range of futures
4. True ambiguity

At level one the residual uncertainty is irrelevant to making information security investment decisions, so professionals can develop a single scenario that is sufficiently precise to form basis for their understanding of key variables for the information security investment calculation. To help generate this, managers can use the standard strategy tool kit: market research, analyses of competitors’ costs and capacity, value chain analysis, Michael Porter’s five-forces framework, and so on. It is not uncommon to also perform a risk analysis on the scenario to identify risks and their probable impact on the potential investment.

At level two, the future can be described as one of a few discrete scenarios. Analysis can’t identify which outcome will actually come to pass, though it may help establish probabilities. Most important, some, if not all, elements of the security investment would change if the outcome were predictable. Here, security professionals must develop a set of scenarios based on their understanding of how the key residual uncertainties might play out:

- Getting information that helps establish the relative probabilities of the scenarios should be a high priority.
- Each scenario may require a different valuation model and individual risk analyses.
- Particular attention should be paid to determine what possible trigger points to monitor closely if the investment is made. This ensures an opportunity for the security professional to act and correct investments as the future is played out over time.

A range of potential futures can be identified at level three. A limited number of key variables define that range, but the actual outcome may lie anywhere within it. There are no natural discrete scenarios. As in level two, some, and possibly all, elements of the security investment would change if the outcome were predictable. This means that each scenario may require a different valuation model and individual risk analyses, and that particular attention should be paid to determine which possible trigger points to monitor closely if the investment is made.

Developing a meaningful set of scenarios is less straightforward in level three, but there are a few general rules to follow:

1. Develop only a limited number of alternative scenarios – no more than four or five
2. Avoid developing redundant scenarios that have no unique implications for the investment decision
3. Develop a set of scenarios that collectively account for the probable range of future outcomes and not the entire range of possible scenarios
4. Always consider to have a status quo scenario of what will probably happen if no investment is made

An example of a level three residual uncertainty BCA approach is the case study of cost benefit analysis of security investment at Ericsson. In that case we see that the professional services firm Ernst & Young, together with the client, identified three alternative scenarios for how the market for certificate use would evolve: The min, max and medium probable
developments. Due to the residual uncertainties on how fast the market would pick-up, all three scenarios were assessed within their own boundaries using three alternative development curves of market penetration: exponential, linear and inverted exponential. At Ericsson all redundant cost variables were removed from the calculations, and a status quo scenario was not developed, as the stakeholders had decided to either outsource or improve its internal operations of the system.

At level four it is virtually impossible to identify a range of potential outcomes, let alone scenarios within a range. Level four situations are quite rare, and they tend to migrate toward one of the others over time. Nevertheless, they do exist. In these rare cases, the risk analysis should be considered an alternative to the BCA.

Irrespective of the residual risk, the security professional need to ensure two results when performing business case analysis:

- Identifying relevant key performance indicators and variables to be used when making the financial calculations
- Identifying a financial metrics model that incorporates the predictions of the scenario (or scenarios) to determine the value of alternative investment strategies

Depending on what main rationale is driving the potential investment in information security, the Business Case Analysis (BCA) may be more or less relevant to the cost benefit analysis.

<table>
<thead>
<tr>
<th>Main Rationale</th>
<th>Probable relevance to CBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate risk in current control environment</td>
<td>Low</td>
</tr>
<tr>
<td>Business-driven investment require security</td>
<td>High</td>
</tr>
<tr>
<td>measures</td>
<td></td>
</tr>
<tr>
<td>Opportunity for business improvement</td>
<td>High</td>
</tr>
</tbody>
</table>

**Game Theory**

Game theory could enhance traditional decision theory by considering possible behaviour patterns of two or more parties (attackers and defenders). The decision, or decisions, resulting in an optimum of benefit is the best investment. This approach may help security managers to plan security investments in a limited scope of application. The main reason for game theory having a finite practical applicability is twofold:

- If the object for analysis is too large or complex – e.g. many actors involved – the amount of data is difficult to analyse, as the data is based on risk and behaviour analysis and business considerations for all actors and potential scenarios.
- Many information security investments are not considered to mitigate only risks of intentionally illicit acts, but rather managing unintentional risk behaviour (mistakes), unplanned incidents, and other aspects of operational ineffectiveness.

The game theory approach has been used mainly in technical security assessments, e.g. firewall configurations or intrusion detection system design. These types of IT-security solutions are able to identify and analyse both intentional and unintentional behaviour of legitimate users, and attackers, of the enterprise’s infrastructure. In these cases the use of game theories may very well prove to be the most efficient approach to mitigate risks.
Consider the following example provided by Mark Burgess, Professor of Network and System Administration at University College Oslo. A bank offering online banking services needs to authenticate its users to keep their information protected. The bank can use a number of strategies for this. Similarly an attacker can try to attack in a number of ways, by various strategies. How can a bank defend its transactions best? We look for maximum and minimum “payoff” to the different sides. Let the numbers in the table below be the “estimated relative security” of the different strategies. It is primitive, but it helps to illustrate a formal way of picking the best approach:

<table>
<thead>
<tr>
<th>Online Service</th>
<th>Steal card details</th>
<th>Hijack session</th>
<th>Spoof site (trick user)</th>
<th>Trojan horse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Token</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Soft Certificate</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Biometrics</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Looking at the table from a broad perspective, we see that it pays an attacker to try to spoof or use a Trojan horse, having mostly low scores in those columns, rather than try to steal a key, or hijack a session, where the highest security-scores are found. For the defender, things are not so clear-cut.

If we think “min-max” from the attacker’s viewpoint, then we are minimizing defensive security and maximizing the attackers reward. Minimizing places us in the last two columns, since that is where the security values are lowest and thus the weakest points. From the defender’s viewpoint we should try to prevent these combinations within a system.

<table>
<thead>
<tr>
<th>Online Service</th>
<th>Steal card details</th>
<th>Hijack session</th>
<th>Spoof site (trick user)</th>
<th>Trojan horse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Token</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Soft Certificate</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Biometrics</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

If we instead think “max-min” from a defender’s perspective we maximize defence security first. This places us in the first two columns, with security value 6 (see below). Then we minimize the attacker’s gain. This is no longer so easy, because the columns are not comparable. It looks as though the token-based defence strategy is best (left-hand circle), but only against the first two attack strategies. Against the second two, we see that the certificate is the most effective (right-hand circle).

<table>
<thead>
<tr>
<th>Online Service</th>
<th>Steal card details</th>
<th>Hijack session</th>
<th>Spoof site (trick user)</th>
<th>Trojan horse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Token</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Soft Certificate</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Biometrics</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Now we are not quite sure whether the weakness against some strategies outweighs the strength in the first. It depends on the relative importance, or likelihood of the different attack strategies. Clearly the best possible solution is a mixed strategy, with both token and certificate. This might be considered too expensive for the bank, but those aspects are not taken into consideration in this example.

---

When applying the game theory approach, it is not uncommon to overlook the aspect of what specific key targets and strategic goals of the stakeholders that would be affected by the attack-strategies being analysed. Therefore, the security professional should pay particular attention to the following three aspects:

1. Develop a set of attacks that collectively account for the probable range of attacks and not the entire range of possible attacks
2. Getting information that helps establish the relative probabilities of different attack strategies (or level of difficulty to perform such attacks) should be a high priority.
3. Identifying relevant key performance indicators and variables to be used when making the financial calculations

Using game theory to meet the main rationale for the potential investment in information security is unusual, and applies only to certain cases of cost benefit analysis.

<table>
<thead>
<tr>
<th>Financial Performance Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Metric</strong></td>
</tr>
<tr>
<td>ROI (ROIC)</td>
</tr>
<tr>
<td>NPV</td>
</tr>
<tr>
<td>IRR (MIRR)</td>
</tr>
<tr>
<td>FCF</td>
</tr>
<tr>
<td>DCF</td>
</tr>
<tr>
<td>Payback Period</td>
</tr>
<tr>
<td>TCO</td>
</tr>
<tr>
<td>TBO</td>
</tr>
<tr>
<td>EVA</td>
</tr>
<tr>
<td>ROSI</td>
</tr>
</tbody>
</table>
The security professional developing the CBA should aid the decision makers by addressing relevant financial performance metrics of the organisation. If the main value discipline is operational excellence, the CBA should focus on asset utilisation, while organisations driven by customer intimacy will have greatest success using CBAs that focus on profit. In organisations focused on product leadership, should aim the financial metrics of the CBA at identifying potential for growth.

Depending on which main value discipline is driving the potential investment in information security, the different financial formulas may be more or less relevant to the cost benefit analysis. Some formulas are clearly focused on one of the value disciplines, e.g. neither TCO nor Payback Period consider profits, while EVA reflects growth by value-add to shareholders only. Despite this, there are no clear-cut lines between the majority of different calculations. As an example, a profit identified via positive free cash flow (FCF) allows an enterprise to pursue opportunities that could enhance shareholder value, which obviously gives opportunities for growth.

### Main Value Disciplines and Financial Metrics

These aspects need to be considered not only during the financial calculations, as the use of non-financial metrics help to identify and quantify key performance indicators and variables used in the financial part of the CBA. As a result, the security professional needs to perform the non-financial and financial parts of the CBA iteratively to be able to identify and capture value to the stakeholders and formal investment decision makers.

The iterative process of using financial calculations and non-financial metrics are critical to success in this work.

The security professional performing the CBA needs to use the underlying key strategies and goals, and available input data from the non-financial metrics to find a suitable set of formulas:

- What main value disciplines drive the investment (asset utilisation, profit or growth)
- What are the key strategies and goals (identify key performance factors)
- Iteratively: Input data and useful financial formulas (see illustration below)

Once the financial metrics have been identified, the actual calculations are seldom challenging to a professional with a financial background. As the mathematical part is often quite easily
handled, requiring only the input of e.g. cash flows and discount rates into a spreadsheet and the rest is a done deal; seldom there is a template available per se.\textsuperscript{127}

**Validation of the CBA**

The last step of the CBA is to validate that it meets the expectations of the stakeholders and the needs of the enterprise. In good corporate governance management oversees the enterprise’s portfolio of investments and manages the required cash flow and risk exposures. Portfolio management enables decision makers to align their portfolios with enterprise strategy and balance risk and returns. The portfolio concept assists managers in balancing and realigning their investments when the enterprise’s strategy or the economic climate changes. The decision makers track a series of financial metrics to manage the enterprise’s assets, intervening only if there are problems or unforeseen opportunities. Similar principles apply to who can commit the enterprise to a contract or a partnership.

When validating the information security investment the security manager will find it useful to think of the enterprise’s information security investment as part of the ordinary portfolio of investments in the enterprise. Portfolio management enables decision makers to align their portfolios with enterprise strategy and balance risk and returns. We need to understand how the proposed investment will fit with the decision makers’ key strategies and goals:

1. What process changes or enhancements that are strategically important are included in the proposed investment?
2. What are the distributions in the current and proposed project portfolios? Will the acceptance of this investment keep the portfolios consistent with the enterprise’s strategic objectives?
3. What is the relative importance of enterprise-wide versus business unit investments? Does the proposed investment reflect their relative importance?

\textsuperscript{127} Discussed in e-mail conversation on the topic with Kamal Parmar (employee at Ernst & Young Kenya), who is a published author on the subject of information security cost benefit analysis: Parmar, Kamal, 2007. Accessed 2007-06-17
RECOMMENDATION

The purpose of this thesis is to present an approach for good practice with regards to using cost benefit analysis as a value-adding activity in the information security investment process for large enterprises.

The thesis is aimed at being valuable to information security professionals responsible for investments in information security and to suppliers of information security services or products who want to better meet the needs of the customer companies.

The findings are summarised in a suggested good practice for cost benefit analysis of information security investments. After the suggested good practice has been presented, a final section concludes the thesis, in which the author gives his reflections on its strengths and weaknesses and results yielded during the preparation of the thesis. The author also points out potential areas for further research in the area.

The suggested good practice gives an intuitive step-by-step method for performing cost benefit analyses. Its added value consists of combining generally accepted practices into a comprehensive approach including standard financial calculations, offering comparable measures between information security and other investments of an enterprise. It is supported by empirical data.

However, cost benefit analyses carry a flaw that can easily prove fatal: Costs and benefits must be quantified in the same currency. While this is easy when considering revenue-generating investments – money-in versus money-out – in the information security world this is hard because, although money goes in, what comes back is sometimes hard to express in financial values. Therefore, the reader should keep in mind that a cost benefit analysis, because it demands a common currency, is forever and always at risk of slipping an infinite numerator or a zero denominator into those ratios.128

In order to avoid the risk of such miscalculations the security professional performing cost benefit analyses need not only information security expertise, but also a good working knowledge of financial calculations.

---

128 Geer, Daniel E. Jr., 2001, p2
Suggested Good Practice for CBA of Information Security Investments

This is the summary overview of a good practice approach with regards to using cost benefit analysis as a value-adding activity in the information security investment process for large corporations.

The approach is based on a combination of research theories and supporting empirical data presented in this report, and the experience of the author.

Consider the following approach:
1. Understand main rationale for the security investment
2. Identify stakeholders and strategic goals
3. Perform Cost Benefit Analysis (non-financial and financial performance metrics)
4. Validate that the results are relevant to stakeholders and strategic goals

Good practice in performing CBA of information security investments

By applying the four-step approach, potential information security investments made by large corporations could be managed in a structured way, with financial calculations supporting (or opposing) the proposed investment in relation to other competing investment requests.

There are several benefits of the suggested approach:
- Covering many types of information security investments – ranging from governance process implementations or outsourcing of functions to IT-infrastructure investments
- Providing means to present comparable measures between these and other investments in an enterprise, that make sense to decision makers and stakeholders
- Supported by research and practices in the market
Step 1 – Understand Main Rationale
The investment process starts when the security manager has an identified need for risk mitigation. The main rationale for these needs vary, and have different implications on what methods to use to perform a useful CBA.

<table>
<thead>
<tr>
<th>Main Rationale</th>
<th>Key questions to address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate risk in current control environment</td>
<td>What business values are at stake?</td>
</tr>
<tr>
<td></td>
<td>Who decides which risk level should apply?</td>
</tr>
<tr>
<td>Business-driven investment require security measures</td>
<td>What are the targets for the business-driven investment</td>
</tr>
<tr>
<td></td>
<td>Who decides which risk level should apply?</td>
</tr>
<tr>
<td>Opportunity for business improvement</td>
<td>What types of improvement effects are anticipated (asset utilisation, profitability or growth)?</td>
</tr>
<tr>
<td></td>
<td>Who decides which risk level should apply?</td>
</tr>
</tbody>
</table>

Step 2 – Identify stakeholders and strategic goals
The security manager needs to address the correct stakeholders in order to avoid lack of investments where needed. The stakeholders are both formal investment decision makers and indirect influencers. The enterprise’s archetype governance model should be clarified:

<table>
<thead>
<tr>
<th>#</th>
<th>Archetype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business Monarchy</td>
<td>Top management of the enterprise</td>
</tr>
<tr>
<td>2</td>
<td>IT Monarchy</td>
<td>IT specialists</td>
</tr>
<tr>
<td>3</td>
<td>Feudal</td>
<td>Each business unit makes independent choices</td>
</tr>
<tr>
<td>4</td>
<td>Federal</td>
<td>Combination of the group functions and the business units with or without IT involved</td>
</tr>
<tr>
<td>5</td>
<td>IT Duopoly</td>
<td>IT group and one other group (i.e. top management or business unit leaders)</td>
</tr>
<tr>
<td>6</td>
<td>Anarchy</td>
<td>Isolated individual or small group decision making</td>
</tr>
</tbody>
</table>

Before the CBA is performed, the following questions should be considered:
- Who will make the formal investment decision?
- Who will fund the investment?
- What other stakeholders could have an impact on the decision?
- What are the key targets and strategic goals for these stakeholders?

The security professional need also to ensure that the formal performance factors of the investment are considered in the cost benefit analysis:
- Identify performance factors formally evaluated in the investment decision

Step 3 – Perform Cost Benefit Analysis
There are four different types of metrics that complement each other: governance effectiveness, risk analysis, business case analysis (BCA) and game theory. In order to perform the actual cost benefit calculations, the security manager uses the methods or non-financial performance metrics that seem best suited for the specific investment analysis.

<table>
<thead>
<tr>
<th>#</th>
<th>Performance metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Governance effectiveness</td>
<td>Defines how well the solution is aligned with the enterprise’s governance principles</td>
</tr>
<tr>
<td>2</td>
<td>Risk Analysis</td>
<td>Defines risks, probability and potential business impact if realised</td>
</tr>
<tr>
<td>3</td>
<td>Business Case Analysis</td>
<td>Describes future state, or states, for the suggested solution and its environment</td>
</tr>
<tr>
<td>4</td>
<td>Game Theory</td>
<td>Defines alternative strategies for attackers and defenders of information</td>
</tr>
</tbody>
</table>
The security manager needs to identify what non-financial metric, or combination of metrics, to use in order to capture the stakeholder values previously identified.

<table>
<thead>
<tr>
<th>Main Rationale</th>
<th>Metric</th>
<th>Probable relevance to CBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate risk in current control environment</td>
<td>#</td>
<td>1, 2</td>
</tr>
<tr>
<td>Business-driven investment require security measures</td>
<td>#</td>
<td>2, 3</td>
</tr>
<tr>
<td>Opportunity for business improvement</td>
<td>#</td>
<td>2, 3</td>
</tr>
</tbody>
</table>

The security professional performing the CBA needs to use the underlying key strategies and goals as well as the available input data from the non-financial metrics to find a suitable set of formulas:

- What main value disciplines drive the investment (asset utilisation, profit or growth)
- What are the key strategies and goals (identify key performance factors)
- Iteratively: Input data and useful financial formulas (see illustration below)

Once the financial metrics have been identified, the actual calculations seldom provide any challenge to a security professional with some financial experience or background.

**Step 4 – Validate that the results are relevant to stakeholders and strategic goals**

Before presenting the CBA to the investment decision makers, the security manager should ensure an understanding of how the proposed investment will fit with the decision makers’ key strategies and goals:
1. What process changes or enhancements that are strategically important are included in the proposed investment?
2. What are the distributions in the current and proposed project portfolios? Will the acceptance of this investment keep the portfolios consistent with the enterprise’s strategic objectives?
3. What is the relative importance of enterprise-wide versus business unit investments? Does the proposed investment reflect their relative importance?
Reflections

The aim of the thesis has been to bring value to information security professionals responsible for investments in information security and to suppliers of information security services or products who want to better meet the needs of the customer companies.

The author has presented research in the field of good corporate governance and the investment process, as well as given case studies from two multinational enterprises. The case from Motorola demonstrated how IT governance principles are equally applicable to information security governance. The case from Ericsson demonstrated how an information security investment decision could be supported by performing a cost benefit analysis using traditional marketing approaches of business case analysis (BCA) and standard financial calculations.

The author, himself being active in the professional services industry, had several expectations before starting to examine the subject from an academic standpoint. Some of these expectations were confirmed by the research and empirical data, while some were not.

The major anticipation confirmed was the applicability of standard financial calculations for information security investments, making the need for “new” or “unique” ways of measuring security investments obsolete. The information security industry and its practitioners seem to have everything to gain by aligning its practices with accepted good practices regarding any other investments of an enterprise, as shown in the case study of Ericsson.

In the early stages of preparing the thesis, the author strived to find a generally accepted approach for performing cost benefit analyses. Being a practitioner, the author focused on identifying not only research models and intellectual structures for assessing value of information security practices, but to identify models and methods that are being successfully used in the market. One previous notion of the author that was proven wrong during the research phase for the thesis was the expectation to find more published cases on performed cost benefit analyses.

While preparing this thesis, the author has also gained new perspectives on how to measure the less tangible security investments in ways that meet the needs of decision makers and other stakeholders, as shown by research performed by the Massachusetts Institute of Technology’s Sloan School of Management and confirmed by the case study of Motorola.

Based on the literature and Internet research performed, the author has concluded that there is no single generally accepted approach, but rather four complementing families of methods or non-financial performance metrics (governance effectiveness, risk analysis, business case analysis, and game theory) trying to measure different types of information security investments. What seemed to be lacking was the step to connect these with the financial calculations based on generally accepted formulas used outside the security industry.

This provided the foundation for the suggested good practice for CBA of information security investments presented in this thesis.
**Strengths and weaknesses**
The suggested good practice gives an intuitive step-by-step method for performing cost benefit analyses. Its added value consists of combining generally accepted practices into a comprehensive approach, offering comparable measures between information security and other investments of an enterprise.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covers many types of information security investments, ranging from governance process implementations or outsourcing of functions to IT-infrastructure investments.</td>
<td>Requires both information security expertise and good working knowledge of financial calculations to be able to perform proper analyses.</td>
</tr>
<tr>
<td>Provides means to present comparable measures between these and other investments in an enterprise that make sense to decision makers and stakeholders.</td>
<td>Few published case studies available. With more cases available, the suggested good practice could be further refined or adjusted according to those findings.</td>
</tr>
<tr>
<td>Supported by research and generally accepted market practices.</td>
<td>Not suitable for small and medium enterprises due to the time and resources required to perform CBA.</td>
</tr>
</tbody>
</table>

**Further research**
The author believes it would be of value to the information security industry if further fieldwork-based research would be performed in the area.

Specifically the following areas could be of value:
1. Creating industry methods and templates for performing cost benefit analyses
2. Performing cost benefit analyses and collecting CBA benchmark data
3. Refining the suggested approach based on stakeholder interviews and benchmark data

**Final Note**
The author would like to thank the following individuals for their contributions to this thesis: Anders Wiger, Ann-Christin Cardholm, Fred Kudrén, Kamal Parmar, Oddgeir Hvidsten, Stig Sörling, Örjan Edberg.
Sources

PRINTED SOURCES


Berinato, Scott. *Finally a real return on security spending*. Framingham (MA): CXO Media Inc., 2002


ONLINE SOURCES


ILLUSTRATIONS

Effectiveness of IT Governance

Five Basic objectives of information security management


Governance Arrangements for 256 enterprises

Information Security Governance at Motorola


Relative development curves for lowest/highest penetration of certificates

Sample Risk Analysis Heatmap

Scope of IT Governance and Information Security Governance

The Governance Arrangements Matrix

The MIO Matrix,
Eriksson, Hauer and Hultén, 2004//Mind Map Marketing-a creative approach to developing marketing skills

Three Value Disciplines