CHAPTER FIVE:
BUSINESS VALUE OF INFORMATION SECURITY GOVERNANCE

5.1 Structure of chapter

Information security practitioners are generally astounded at director's and top management's perception of, and attitude towards, information security governance.[1] Moreover, they find it difficult to understand why top management is struggling to come to grips with the question why information security needs to be governed in the first place. [2] For information security practitioners the answer to this question is self-evident, unfortunately this answer still evades top management.

The reluctance and apprehension with which this subject-matter is approached manifests itself in various ways, ranging from inadequate resources allocation to a general lack of follow-through and commitment to information security efforts. The reason for the reluctance lies in director's and top management's inability to visualise the business value of information security governance.

Their reluctance is however, to a certain extend, justified when considering the difficulties they encounter when wanting to determine the business value of information security, namely:

(i) Benefits delivered by information security are generally of an intangible nature, and therefor inherently hard to place a monetary value on. Therefore the challenge lies in "finding the tangible equivalents of intangible benefits,"[3] combine this with the fact that

[1] Tipton and Krause *Information Security Management Handbook* Vol 2 (2001) 241.
[2] ibid.
[3] Unknown "Measuring IT value" (last visited 18 November 2002) http://www.cio.com/CIO/022101_survey.html 1.

information security is not used solely in one department, unit or application of which the performance may be measured; [4] and

(ii) It is hard to illustrate how information security functions as a business enabler and supporter.[5]

Accordingly, the essence of these two problems may be captured by the following two questions:

(i) What value does information security deliver to the organisation? and

(ii) How does information security support and enable the organisation?

Fortunately, solutions to both seemingly intractable, complex information security problems exist.

The solution to the **first question** comes in the form of a performance measurement system, and specifically the development of a balanced scorecard, which will aid the organisation and board members alike in: (i) convincing them of the need for information security; and (ii) justifying current and future investments in information security.

The **second question** highlights the importance of ensuring that the organisation and information security, respectively are moving in the same direction.[6] Therefor information security's mission, goals and objectives should be in harmony/aligned with the overall organisational mission, goals and objectives. Misalignment will result in "inappropriate investment decisions; badly chosen priorities and the delivery of the

[4] Van Gremberger and Amelinckx "Measuring and managing e-business projects through balanced scorecards" (last visited 8 February 2002) http://www.ITgovernance.org 1.

[5] Williams "Value versus cost: governing IT on a reduced budget" (last visited 11 May 2002) http://wwwComputerWeekly.com 2.

[6] ibid.

desired results will not be achieved.”[7] Strategic alignment will therefor provide the answer to the second question.

Any attempt to make a business case for information security governance will therefor have to involve two activities: (i) performance measurement; and (ii) strategic alignment.

Outline of chapter:

This chapter is subdivided into four parts:

Part 1: will discuss director’s and management’s perspective on information security;

Part 2: will discuss performance measurement, by addressing five pivotal questions:

(i) Why measure performance in information security?

(ii) What is performance measurement?

(iii) How does performance measurement function as a business enabler?

(iv) How to develop a performance measurement system? and

(v) What does the balanced scorecard methodology entail?

Part 3: will discuss strategic alignment by addressing the following three questions:

(i) What is strategic alignment?

(ii) Why does the need for strategic alignment exist? and

(iii) How does strategic alignment function in the information age?

Part 4: will indicate the business value of information security governance.

[7] Duffy “Alignment: delivering results” (last visited 26 September 2002) http://www.cio.com 3.

5.2 PART ONE: TOP MANAGEMENT'S PERSPECTIVE OF INFORMATION SECURITY

When attempting to "sell" information security to directors and top management the following should be kept in mind:

(i) Directors and top management are faced with a multitude of problems and risks on a daily basis. [8] Information security is just another one of them.

(ii) Directors and top management are inclined to oversimplify the information security problem. [9] They feel that it is the IT department's responsibility to ensure that authorised users are allowed access to information, and that unauthorised users should be denied access. [10]

(iii) When wanting to communicate the value information security holds for the organisation this value must be translated into business terms. Therefor "speaking in managerial terms is key." [11] There exists a general lack of understanding, appreciation and sufficient insight into the inherent value of information, not only amongst top management, but also lawyers, accounts and financial advisors of the organisation.[12]

(iv) The reluctance with which investments in information security are approached is a direct result of the exaggerated problems anticipated with Y2K, which resulted in organisations dissipating their IT budgets for the

[8] (n 1) 242.

[9] ibid.

[10] ibid.

[11] ibid.

[12] Unknown "Prevent abuse, theft of intangible assets through better management" (last visited 18 April 2002) http://www.computingsa.co.za/2002/04/15/News/new09.htm1.

next ten years. [13] The lack of serious problems resulting from Y2K fostered a "cry-wolf" attitude amongst top management. Consequently, organisations feel that the issue of information security has been overdone.[14] "They have heard it so often that they have become incurred to it. Information security is not news any more."[15] However, top management must be mindful of the fact that there exists one big difference between the Y2K problem and the information security problem, namely that Y2K was a static problem for which a workable solution could be developed.[16] Unlike Y2K information security may be compared to a living, breathing and ever-evolving organism. [17] Consequently as observed by Opperman:[18]

> "The complexities associated with Y2K pale into significance when compared to the imminent information security crisis…one is dealing with an 'enemy' that is increasing not only in intelligence, but also in numbers."

(v) Top management takes a dollar-to-dollar approach to information security. [19] Therefore, for every dollar spent on information security they expect to see this amount being delivered back to the organisation in the future.[20] However, most of the benefits delivered by information security materialise in the form of increased efficiency, effectiveness, and productivity, leverage the competitive advantage, and improve the value proportion, therefor not being expressed in dollars and cents. [21]

[13] (n 1) 242.

[14] Melamed "Total onslaught on information security" (last visited 18 February 2002) http://computingsa.co.za 2.

[15] ibid.

[16] Opperman "ISIZA reports back from the global information security (InfoSec) summit" (last visited 18 April 2002) http://www.itweb.co.za 1.

[17] ibid.

[18] ibid.

[19] Pender "How to communicate value" (last visited 18 November 2002) http://www.cio.com/archive/010101/value_content.html? 4.

[20] ibid.

[21] ibid.

(vi) Top management still views the information security unit/department of the organisation as a cost center, rather than a value center.[22]

Consequently, directors and top management must be convinced of the business value information security governance will hold for their organisation.

[22] (n 3) 1.

5.3 PART TWO: PERFORMANCE MEASUREMENT – DEFINING THE VALUE OF INFORMATION SECURITY

5.3.1 Introduction – the need for performance measurement [23]

"Performance measures define the management information you need to make decisions and to determine what is success and failure." [24]

One of the most important issues confronting top management at present is the intense focus on results. In the current economic environment it is expected of organisations to become more result-orientated. Shareholders insist on being provided with concrete facts on the performance of the organisation as a whole as well as on departmental, unit and even project level. Shareholders demand to know what they are receiving in return for their investment in the organisation. If these benefits are unclear they will simply stop injecting money into the oganisation.

All projects undertaken, especially those relating to information security require a high level of resource investment such as time, money and skilled personnel. [25] It is the goal of every organisation to allocate its available resources as effectively as possible in order to generate a large profit and ensure maximum return on investment (ROI) for shareholders.

[23] The importance of performance measurement may be illustrated by the fact that in the United States of America performance based management is of such crucial importance that congress have enacted several pieces of legislation which requires of government executives to clearly define their missions and goals, implement effective performance measurement and report on the results. Amongst these pieces of legislation we find Chief Financial Officers Act (CFO) of 1990; Government Performance and Result Act (Result Act) of 1993; Federal Acquisition Streamlining Act (FASA) of 1994; Paperwork Reduction Act of 1995; and Clinger-Cohen Act of 1996. Tipton and Krause (n 1) 5-7. At present there does not exist legislation in South Africa that imposes a duty upon an organisation to perform performance measurement.

[24] Statement made by a Chief Information Officer in IT Governance Institute "Board briefing on IT governance" (last visited 18 November 2002) http://www.itgovernance.org 2.

[25] (n 5) 2.

It is therefor of crucial importance to determine if a project delivers what it is suppose to deliver. [26]

Entities charged with the responsibility of information security are faced with a problematic situation: because of the rapid rate at which new technology is developing and present technology becomes old and obsolete it is difficult to justify the cost and evaluate the benefits delivered by information security.[27] A further problem is that information security is not used solely in one department, unit or even application of which the performance may be evaluated on a regular basis. Keep in mind that, as will be discussed in part three of this chapter, information security forms an integral part of the organisation as a whole, and cannot be resected from the organisation without resulting in an all but complete collapse of the organisation itself. As a result of this it is becoming increasingly difficult to estimate the contribution information security is making to the overall business' performance.

One of the biggest problems associated with information security is that most, if not all benefits offered by information security are difficult to measure due to their intangible nature.[28] "Intangible benefits are inherently hard to place a monetary value on and this in turn result in no calculable business value."[29] A monetary value for benefits and cost are however needed in order to justify any future investment and resource allocation in information security. The solution to this problem comes in the form of a performance measurement system, specifically the development of the balanced scorecard which can measure tangible as well as intangible benefits and elements.

[26] (n 5) 1.

[27] (n 19) 4.

[28] (n 5) 1.

[29] Some examples of intangible benefits may include better customer service or a shorter response time.

5.3.2 Defining performance measurement

Performance measurement may be defined as "…a tool to other ends not the end in itself,[30] that: (i) translates organisational vision into operational and quantifiable measures; (ii) reduce a strategy to its critical success factor; and (iii) creates organisational and individual alignment."[31] Measurement will indicate how well a department, unit, team or organisation is doing in reaching a given objective, goal or outcome.[32] Measurement[33] also enables the organisation to manage with agility, giving organisations the ability to be more flexible and the advantage of being able to quickly adapt and respond to an ever-changing business environment.[34]

Performance measurement provides answers to the following four pivotal questions:

(i) "What is important in the organisation?

(ii) What does the organisation hold itself accountable for?

(iii) How does the organisation define success? and

(iv) How does the organisation structure improvement efforts?"[35]

5.3.3 Performance measurement as a business enabler

The question may be asked how a measurement system can help an organisation attain its goals?

[30] Keep in mind that performance measurement is only a means to an end and not the end in itself. Because of the fact that performance measurement is a tool the possibility does exist that it may be misused. See the conclusion of part two for suggestions on how to avoid this possibility from becoming a reality.

[31] Fanvielle and Carr "Gaining strategic alignment: making scorecards work " (Fall 2001) *Accounting Management Quarterly* 7.

[32] Chang and Morgan *Performance Scorecards: Measuring the Right Things in the Real World* (2000) 45.

[33] It should be kept in mind that "measurement is a separate discipline from what is being measured" Neuendorf *Project Measurement* (2002) 69.

[34] Rubin "Checks and balances – measuring the value of technology investment: lets get physical" (15 Nov 1998) *CIO Enterprise Magazine* 1.

[35] United States General Accounting Office: Accounting and Information Management Division *Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments* GAO/AIMD-98-89 (March 1998) 5.

(i) Measurement provides an accurate, up-to-date condense picture of the moving key indicators.[36]

(ii) It acts as a warning signal indicating any fluctuations in critical areas that might directly or indirectly impact on the organisation's ability to reach its set goals and objectives. These warning signals will take the form of leading and lagging indicators.[37]

(iii) It translates and then communicates organisational goals, objectives, targets and performance into understandable terms across the whole organisation.

5.3.4 Performance measurement in the information age

The main purpose of the performance measurement program is to illustrate how information security is supporting and enabling the business process.[38] In today's turbulent environment resources are limited and budgets are tight. All decisions surrounding the allocation of resources to, and the investment in, the information security department will depend a great deal on how the information security performs in

[36] Rubin (n 34) 2 puts forth three basic principles of physics that a performance measurement system will utilise to ensure success within the organisation:

(i) "Current status (Positioning);
(ii) Position relative to targets (Direction); and
(iii) Movement towards targets" (Movement)."

[37] (i) Leading indicators - This type of indicator focuses on present as well as future performance, they are forward-looking, as opposed to its counterpart lagging indicators. Predictions on future performance will form the basis of this indicator. An example of a leading indicator may be return on investment (ROI) for shareholders. Within the organisational structure directors and management will look to these indicators when making decisions; (ii) Lagging indicators - This type of indicator focuses on past performance, and will mostly rely on historical records of past performance. An example of this type of indicator may be last year's market share. Shareholders will make use of the results delivered by lagging indicators when making investment decisions. Mayor "Value made visible" (last visited 18 November 2002) http://www.cio.com/archive/050100_method_content.html 3.

[38] Kaydos *Operational Performance Measurement* (1999) 44.

fulfilling expectations and improving its performance.[39] Mayor[40] observes that "for an increasing number of executives and financial officers, vague promises of productivity enhancements and cost cutting are no longer enough to justify ever more voracious budgets (for information security)."

5.3.5 Information security performance measurement objectives

Performance measurement of information security has as its objective the following:

(i) Assist top management in making more informed decisions regarding information security investments and resource allocation;[41]

(ii) Enable the organisation to quickly identify and measure problems, consider alternatives, and decide on solutions; [42]

(iii) Activate, and impact upon the mission, goals and objectives of the organisation; [43] and

(iv) Monitor the progress made, act upon and learn from results delivered by this program. [44]

5.3.6 Developing information security performance measurement

No universally applicable, "one-size-fits-all" approach to information security performance measurement exists. There is however an ever-increasing number of

[39] Ellis "A solution to managing performance in the IT business sector" (last visited 9 September 2002) http://www.itweb.co.za 1.

[40] "Value made visible" (last visited 18 November 2002) http://www.cio.com/archive/050100_method_content.html 3.

[41] (n 38) 143.

[42] ibid.

[43] ibid.

[44] ibid.

valuation methodologies at the organisations disposal, but the methodology approach adopted will differ from one organisation to another.[45] Organisations will do well to examine the approach leading organisations are taking to performance measurement, and then develop a suggested framework.

The United States General Accounting Office has developed the following framework for the implementation of a performance measurement system:[46]

[45] Some examples of these valuation methodologies include:

(i) Applied information economics (AIE): uses scientific and mathematical methods to evaluate the IT investment process;

(ii) Balanced scorecard (BSC): integrates traditional financial measures with three other key performance indicators: customer perspective, internal business process and organisational growth, learning and innovation;

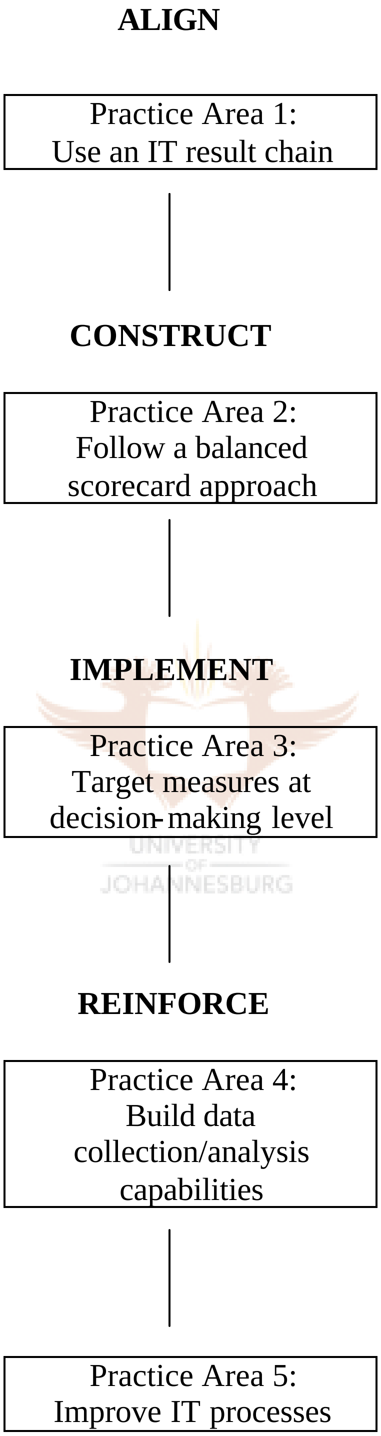
(iii) Economic value added (EVA): calculates 'true' economic profit by subtracting the cost of all capital invested in an enterprise – including technology – from net operating profit;

(iv) Economic value sourced (EVS): quantifies the dollar value of risk and time and adds these into the valuation equation;

(v) Portfolio management: manages IT assets from an investment perspective by calculating risks, yielding and benefits; and

(vi) Real option valuation (ROV): values corporate flexibility above all else; tracks 'assets in place' and 'growth options' to present the widest array of future possibilities Mayor (n 40) 10-11.

[46] For a comprehensive discussion of what each of these practice areas entail, consult United States General Accounting Office: Accounting and Information Management Division "*Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments*" (March 1998) *GAO/AIMD-98-89* 12.


ALIGN
Practice Area 1:
Use an IT result chain
CONSTRUCT
Practice Area 2:
Follow a balanced scorecard approach
IMPLEMENT
Practice Area 3:
Target measures at decision-making level
REINFORCE
Practice Area 4:
Build data collection/analysis capabilities
Practice Area 5:
Improve IT processes

Domain numbers two and four demand specific attention because of the practical value they hold for the organisation.

Domain two, the balanced scorecard (henceforth BSC), has increased in popularity and importance in recent years. A new trend is emerging to develop IT specific, and information security specific BSC's.

5.3.6.1 Overview of the balanced scorecard methodology [47]

Scorecards are increasing in popularity as more and more organisations are beginning to realise the benefits associated with BSC. [48] Not only does it enable the organisation "to manage how their strategy is implemented and measured," [49] but BSC also acts as an alignment mechanism aligning vision with strategy and then ensuring operations can fulfil against the set strategy. [50] It furthermore enables decision makers to focus not only on the financial aspects of the organisation, but also gives managers a view of how strategic decisions will influence staff, customers and the organisational functions as a whole. [51] The balanced scorecard is used to implement a business strategy, by translating the business strategy into performance measures. [52]

The driving force behind BCS was the realisation that when evaluating the performance of a company, a person would be unable to form a complete, accurate and overall picture of that company's performance if he/she only concentrate on the financial aspect thereof,

[47] History of the BSC: The most noteworthy breakthrough in performance measurement occurred in the 1990's with the development of Balanced Scorecards (BSC) by Kaplan and Norton. They defined the original BSC as "…a performance measurement system that supplements traditional financial measures with the criteria that measures performance from three additional perspectives" Williams (n 5) 1.

[48] Jones "Creating the strategy focused IT department" (last visited 23 October 2002) http://www.itweb.co.za 1.

[49] ibid.

[50] ibid.

[51] Robinson "Balanced scorecard" (last visited 18 November 2002) http://www.computerworldcom 1.

[52] Young "Score it a hit" (last visited 18 November 2002) http://cio.com 3.

as was done quite frequently in the past. [53] Other dimensions of the business also needed to be taken into consideration. [54]

5.3.6.2 Information security balanced scorecard

Because of the pivotal role information security plays within the organisation it needs its own scorecard that defines clear goals and good measures that unequivocally reflects the business impact of information security. [55] As a result of this the initial BSC as developed by Kaplan and Norton has in recent years been applied within the information security arena. [56] Consequently, scorecards are now used to accentuate the portentous role information security plays within the context of the organisation as a whole. [57] Information security will no longer be seen as being detached from the organisation, but its performance will be measured across the organisation in its entirety indicating the direct impact or lack thereof information security has on the organisation. [58] BSC furthermore enables the organisation to capitalise on, and employ information security to its full potential. [59] Because of BSC's inherent function to assess performance, it provides a control measure to the board which they can use when dealing with crucial issues such as information security expenses, user satisfaction, expertise of staff, and efficiency of development and operations. [60]

BSC should ultimately demonstrate the value information security delivers to the organisation. [61]

[53] Grindley *Managing IT at Board Level* (1995) 1.

[54] ibid.

[55] IT Governance Institute "Board briefing on IT governance" (last visited 18 November 2002) http://www.ITgovernance.org 22.

[56] (n 5) 1.

[57] (n 39) 1.

[58] (n 39) 2.

[59] (n 39) 1.

[60] (n 5) 3.

[61] See Annexure B for an example of a "Scorecard Checkup."

5.3.6.3 Benchmarking

Domain number four, building data collection/analysis capabilities, involves a concept, which flows from, and is very tightly bound to the notion of a balance scorecard, namely benchmarking. [62] Benchmarking is used to set information security performance targets. It may be defined as "objective measures of performance". [63]

Benchmarking has as its point of departure the assumption that the "investment in the infrastructure is justified, but only to the extend that it is properly managed."[64] Benchmark enables an organisation or department to compare (benchmark) itself against the leaders in a similar field,[65] as there is no point in comparing one to oneself. Therefor, organisations need to know how they compare to their rivals. Benchmarking allows organisations to collect information on organisations "which demonstrate outstanding performance in the areas to be benchmarked."[66] This information will then be analysed and dissected in order to aid in the evaluation, re-design and refinement of existing practices. [67]

By making use of benchmarking organisations are able to compare their own performance to that of:

(i) Other organisations, [68] or

(ii) Similar processes within the organisation, [69] or

(iii) The average for the industry. [70]

[62] Benchmarking originated from the Japanese concept of *dantotsu* which means striving to be "the best of the best." For an overview of benchmarking see Annexure C.

[63] Turban, McLead, and Wetherbe *Information Technology for Management: Making Connections for Strategic Advantage* (1999) 570.

[64] ibid.

[65] Benchmarking should not be confused with baselining. Although these two concepts support each other, their functions are inherently different. Baseline may be defined as a method that "assesses what performance information they had for the measures they had selected." Baseline may be viewed as an initial reference point. It states "where you come from." Without a baseline you will have no standard against which to measure progress. Baselining must form part of BSC, as it is an important action in the performance measurement process that measures the organisation's current performance. Kaydos (n 38) 146.

[66] Watson *Data Management* (1996) 41.

[67] ibid.

[68] (n 35) 53.

[69] ibid.

[70] ibid.

In short benchmarking may be seen as a comparison of performance taking into account averages for the industry and indicating how well the organisation is using its infrastructure.[71] If the performance of an organisation is below standard benchmarking will focus the attention on this problem to allow for corrective action to be taken. A word of caution may be appropriate here: the key to successful benchmarking lies in the fact that organisations should benchmark themselves to similar organisations,[72] therefor look for organisations that have "similar range of business, competing in similar segments and be of a reasonable comparable size and geographical spread."[73]

Unfortunately, as with performance measurement in general, there exists no universally applicable "one-size-fits-all" benchmark. [74] The benchmark needs to be tailor made for the organisation. Therefor organisations must make a conscious effort not to imitate but rather innovate. The way in which organisations answer the following questions will influence the design, implementation and sustainability of the benchmark:

(i) What is the organisational culture?[75]

(ii) How prominent/important is information security within the organisation to mission delivery?[76]

(iii) What is the acceptable utility of information security in the organisation? [77]

[71] (n 63) 570 – 571.

[72] Scott *Value Drivers* (1998) 245.

[73] ibid.

[74] (n 39) 2.

[75] This question focuses on whether or not top management supports information security performance measurement and whether this support is reflected in reward programs, incentive schemes or appraisals offered to personnel. The most important factor when dealing with performance measurement, specifically benchmarking, is top management involvement. But the term "involvement" might be misleading. In this context involvement encompasses ownership as well as the use of results delivered by performance measurement to take corrective measures. Ownership needs to be fostered throughout the organisation. Kaydos (n 38) 57-58.

[76] (n 39) 2.

[77] ibid.

(iv) Who is assigned responsibility for information security and on what level in the organisation (central/managed/dispersed)? [78] and

(v) What resources are available to support information security not only in the form of financial resources, but also in the context of skills, people and tools?[79]

Two forms of benchmarking is encountered, namely:

(i) Metric benchmarking; [80] and

(ii) Best practice benchmarking. [81]

(i) Metric benchmarking

Metric benchmarking represents a numeric performance measurement system. [82] Some examples of this form of benchmarking may include:

(a) Information security expenses as a percentage of the total revenue;[83]

(b) Percentage of downtime; and [84]

(c) Percentage of information security projects completed on time and within budget. [85]

This form of benchmarking is important and has significant value for managers as it helps to identify problems. The difficulty associated with this form of benchmark is that it identifies the problem, but does not necessarily solve the problem. In order to find a solution for this problem organisations need to look to the second form of benchmarking, namely best practice benchmarking.

[78] ibid.
[79] ibid.
[80] (n 63) 570.
[81] ibid.
[82] ibid.
[83] (n 63) 571.
[84] ibid.
[85] ibid.

(ii) Best practice benchmarking [86]

Best practice benchmark places the emphasis on how information security activities are actually performing rather than focussing on numeric performance measures.[87] It is suggested that rather than choosing and then focusing on one form of benchmarking organisations should utilise both these forms in conjunction with one another.

Ultimately, benchmarking will aid organisations in identify "gaps" between expected results and actual results delivered.

5.3.7 Conclusion

Because of the problems associated with benefits delivered by information security a performance-based, result-orientated, decision-making approach to information security investments are needed. A starting point is to build credibility for the value of information security within the organisation. Therefor, an investigation needs to be launched into how effectively information security is being utilised within the organisation, and how this can be improved. Through an effective performance measurement program management will be convinced of the value of information security in the organisation and they will have documented proof which they can use to justify past, present and future investments in information security. "Without the ability to measure performance, a company cannot be sure that it really is protecting its information assets as well as it thinks it is."[88]

[86] ibid.

[87] ibid.

[88] KPMG "Global information security survey" (last visited 18 November 2002) http://www.kpmg.co.uk 3.

It would be appropriate at this time to give a word of caution: " no organisation has ever measures itself into excellence"[89] There exist no single performance measurement system or technique that will make the organisation a success. BSC is just one of multifarious measurement tools used to motivate change, but it does not tell the organisation how to change. All measurement systems need to be linked to physical action that drives the change. It is contended by Brimson[90] that managers can no longer rely on the archaic believe that if they introduce measurement tools people are clever enough to figure out what to do with it all by themselves. It is a well-known fact that tools and training go hand-in-hand. Even the best developed performance measurement system will fail if people do not receive the necessary training on how to implement the system.[91]

[89] "Why your balanced scorecard will not be successful – unless" (last visited 18 November 2002) http://www.bettermanagement.com 2.

[90] (n 89) 1.

[91] ibid.

5.4 PART THREE STRATEGIC ALIGNMENT

5.4.1 Introduction

The next issue that the board will have to address is whether or not the organisation's investment in information security is in harmony with the organisation's strategic objectives. In the information age it is required of top management to understand how information security supports, enables and fits into the organisational strategy as a whole.[92] Top management must be able to answer the following questions with confidence, in order to discharging their responsibilities effectively:

(i) What are the implications of information security in my business operations? Today? In the future? [93]

(ii) What are the alternative perspectives for leveraging information security capabilities for business operations? [94]

(iii) Is the locus of information security competence "inside" or "outside" the operation? [95]

(iv) What is the executive role of senior management for leveraging information security capabilities? [96]

(v) How should the information security function be organised, and what is the role of information security outsourcing? [97] and

(vi) What are the appropriate criteria for assessing information security-based benefits?[98]

[92] Henderson and Venkatraman "Strategic alignment: leveraging information technology for transforming organisations" (1993) *IBM Systems Journal* Vol 32 no 1 5.
[93] ibid.
[94] ibid.
[95] ibid.
[96] ibid.
[97] ibid.
[98] ibid.

These questions accentuate why the need to ascertain whether or not information security is "moving" in the same direction as the overall business, exist. This would imply tha t the information security strategy must not only support, but also enable the organisation's overall strategy, thereby creating harmony/alignment between the two. Part three will therefor focus on how to align the information security strategy with the overall organisational strategy thereby ensuring that information security contributes and enables the organisation to reach its ultimate goals and objectives.

5.4.2 The concept of corporate strategy [99]

The essence and need for strategy within an organisation can best be illustrated by the scene in "Alice in Wonderland" where Alice comes to a crossroad and ask her companion "Which road do we take now?" he replies "Well, where do you want to go?" to which Alice answers "I don't know." In his reply lies the essence of strategy "If you don't know where you want to go, it really doesn't matter which road you take."[100] An organisation without a strategy may be compared to the position Alice finds herself in: if they do not know where they want to go, then where they are and where they have been is irrelevant.

[99] It is contended by Ernst and Young that two of the most pivotal issues on which investors want information is in the first place, how effectively the organisation is executing its strategy, and secondly the quality of the strategy. Wixley and Everingham *Corporate Governance* (2003) 10.

[100] Puth *The Communicating Leader* (2002) 180.

5.4.3 Defining strategy [101]

Strategy is one of the most abused words in the business lexicon. Boar[102] views strategy as "…the definition of both what is to be accomplished and the means of accomplishment."[103] Hickman and Silva[104] are in favour of a working definition for the term strategy which involves outthinking, outplanning and outplaying the competition. Keep in mind that each business strategy should be unique, as all organisations are influenced and shaped by different internal and external forces that will inevitably have an impact on its strategy.[105]

Therefor strategy should be seen as a multidimensional discipline which includes, amongst other thing **decisions** about:

(i) "What business the company should be in;

(ii) Who its customers are; and

(iii) How it will measure success."[106]

and **activities**[107] on:

[101] Some writers draw a distinction between corporate strategy and business strategy. For the purpose of this discussion this distinction is not of pivotal importance, and will therefor not receive much attention. Andrews T*he Concept of Corporate Strategy* (1987) 13 defines these two concepts as follow: corporate strategy is "…the pattern of decision in a company that determines and reveals its objectives, purposes or goals, produces the principal policies and plans for achieving those goals, and defines the range of business the company is to pursue, …and the nature of the economic and non-economic contribution it intends to make its shareholders, employees, customers, and communities...". It therefor defines the business in which a company will compete, and is applicable to the organisation as a whole. Whereas business strategy may be defined as "…the determination of how a company will compete in a given business and position itself amongst its competitors."

[102] *The Art of Strategic Planning for Information Technology* (2001) 36.

[103] (n 102) 227.

[104] *Creating Excellence: Managing Corporate Culture, Strategy, and Change in the New Age* (1984) 41.

[105] Andrews *The Concept of Corporate Strategy* (1987) 22.

[106] Wixley and Everingham *Corporate Governance* (2003) 10.

[107] Osgood "The strategy alignment model: defining real estate strategies in the context of organisational outcomes" (last visited 9 September 2002) http://www.siteselection.com 2 identifies the following five building blocks of strategy:

(i) Mission for today and vision for the future;
(ii) Customers and markets served;
(iii) Products and services offered;
(iv) Distinctive competencies or skills unique to the company; and
(v) Values and culture that serves as the foundation for any organisation.

(i) “Setting objectives;

(ii) Deciding on a mission or purpose;

(iii) Evaluating the environment within which it must operate;

(iv) Defining its key stakeholders;

(v) Determining its competitive advantage; and

(vi) Formulating detailed strategies to accomplish its aims. ” [108]

A primary **objective** of a strategy should be to develop “a highly adaptive and maneuverable business so that the day-to-day business process can maintain a strategic fit with the environment.”[109] Strategy is more than just action.[110] Boar[111] is of the opinion that the essence of strategy lies in “the eternal struggle for business, is the struggle for advantage. The one with more advantage wins; the one with fewer advantage loses. Strategy is the careless pursuit of advantage.”

Puth[112] identifies three basic elements of strategy namely:

Strategy will answer the following questions:

(i) The place that we want to go;

(ii) The place where we are now; and

(iii) The journey from here to there. [113]

Characteristics of a strategy include:

(i) Forward looking; [114]

(ii) Deals with long-term issues; [115]

[108] (n 106) 10.
[109] (n 102) 273.
[110] (n 102) 236.
[111] (n 102) 4.
[112] (n 102) 180.
[113] ibid.
[114] (n 102) 273.
[115] ibid.

(iii) Anticipate/forecast; [116] and

(iv) Flexible and easily adaptable. [117]

Strategy development consists of two primary **building blocks** or components, namely:

(i) Strategy formulation; [118] and

(ii) Strategy implementation. [119]

A strategy scorecard may proof valuable in the evaluation process in order to measure the effectiveness of the strategy and identify areas in which urgent attention is needed.[120]

5.4.4 Defining alignment

Puth[121] views alignment as "…the measure to which everyone in the organisation expends his/her energy in the same direction." "Alignment means that behaviour throughout the organisation is directed towards the achievement of shared goals. Through clear objectives and commonly shared vision, alignment keeps an organisation focused."[122]

Alignment is a holistic discipline, which is based on two important assumptions:

(i) "The term strategic alignment presupposes that there is a strategic line (a) a clear overall strategic direction, intent, and set of desired outcomes; (b) that business units, divisions, and eventually every individual can align their action to; and

[116] ibid.

[117] ibid.

[118] For a detailed discussion on strategy development and implementation, consult Wixley and Everingham *Corporate Governance* (2003) 11-12; and Andrews *The Concept of Corporate Strategy* (1987) 81-82; 91.

[119] (n 106) 11-12.

[120] For an example of an information security strategy scorecard see Annexure D.

[121] (n 100) 201.

[122] (n 100) 211.

(ii) Everyone is aware of this strategic line and that it is sufficiently "visible" for alignment to take place."[123]

5.4.5 Importance of strategic alignment

"A misaligned strategy is equivalent to an incorrect map. Following it can lead to wrong turns and delays if not downright disaster."[124]

The question may be asked why it is required of the board to concern itself with strategic alignment. The answer to this question is two-fold: (i) strategic alignment acts as an enabler of the organisation, and (ii) numerous benefits are attached to the strategic alignment process.

Benefits of strategic alignment:

(i) Strategic alignment:

(a) "provides a methodology for developing high level strategy which is customer led";[125]

(b) will ensure that the strategy is clearly articulated and understood by all while simultaneously assigning roles and responsibilities for the formulation and implementation of the strategy, thereby removing any uncertainty that may have existed about responsibilities;[126]

(c) will enable the organisational strategy to cascade down to all levels of the organisation in order to inform all employee thereof, and educate them thereon;[127] and

[123] (n 100) 198.
[124] Fitz-endz *The E-Aligned Enterprise* (2001) 75.
[125] Novaconnection "Strategic alignment" (last visited 12 October 2002) http://www.novaconnection.com 1.
[126] ibid.
[127] The Knowledge Company "The case for strategic alignment" (last visited 9 December 2002) http://216.239.51.100/search…/1010268883789.doc+strategic+alignment&hl=en&ie=UTF- 4.

(d) will enable managers to identify and focus on the organisation's strengths and weaknesses,[128] thereby giving them insight into the organisation's capabilities and competencies. [129]

(ii) Strategic alignment enables the organisation to obtain a sustainable competitive advantage as alignment "focuses efforts and attention on the areas which will provide the most effective competitive advantage"; [130]

(iii) Strategic alignment enables the organisation to become more flexible thereby enabling it to adapt and adjust quickly to changes occurring in the business environment. [131] Alignment furthermore "supports the quick and effective evaluation of the impact of changing strategic plans"; [132]

(iv) Strategic alignment abates the required resource investment by reducing the time required, and money needed to realise strategic plans by:

(a) Eliminating redundancies; and

(b) Eliminating conflicting work/projects. [133]

Therefor money is not spend, and time is not wasted on projects, activities or work that do not support the organisational strategy;

(v) Alignment focuses energy, resources and activities on certain key factors that will have the greatest positive effect on the organisation;[134] and

[128] Psychometrics.com "Strategic alignment" (last visited 9 December 2002) http://www.psychometrics.com 1.
[129] (n 127) 4.
[130] ibid.
[131] ibid.
[132] ibid.
[133] ibid.
[134] ibid.

(vi) Alignment "ties the corporate personality and culture, processes, capabilities, competencies, resources and realities collectively to the organisational strategy."[135]

5.4.6 Strategic function of the board

The King II report on Corporate Governance 2002 states that "[the board] is ultimately accountable and responsible for the performance and the affairs of the company." It goes on to observe that "…[T]he charter should confirm the board's responsibility for the adoption of strategic plans…". Therefor one of the most important internal functions of the board is to develop and oversee the implementation of the corporate strategy.[136] In practice however the responsibility for strategy formulation will be vested in executive management and the role of the board will be to debate and question the motivation behind the strategy. [137] It is furthermore expected of the board to approve strategic plans and major strategic decisions.[138]

Within the information security governance sphere it will be expected of the board to drive business alignment by:

(i) Ensuring that the information security strategy is aligned with the business strategy;[139]

(ii) Ensure that information security deliver against strategy, which would entail "delivering on time and within budget, with appropriate functionality and the intended benefits, is a fundamental building block of alignment and value delivery";[140] and

[135] ibid.
[136] (n 106) 11.
[137] ibid.
[138] ibid.
[139] (n 55) 19.
[140] ibid.

(iii) Information security strategy must not only enable the existing organisational strategy, but must also act as a conduit for improving the future organisational strategy.[141]

It is suggested by the IT Governance Institute[142] that alignment requires management to perform the following activities:

(i) Raise awareness amongst top management about the strategic role information security plays within the organisation; [143]

(ii) Clarify the role information security should play in the organisation;[144]

(iii) Monitor the impact information security has on the organisation as a whole;[145] and

(iv) Evaluate benefits delivered by information security.[146]

To aid the board in discharging the multitude of onerous responsibilities and duties that this component places on them, the researcher recommends that an Information Security Strategy Committee should be established.[147] The function of this committee would be to aid the board in aligning the information security strategy and related matters with the overall organisational strategy.[148]

[141] ibid.

[142] ibid.

[143] ibid.

[144] ibid.

[145] ibid.

[146] ibid.

[147] See Annexure E for a framework on how to develop, form and incorporate an Information Security Strategy Committee.

[148] It should be kept in mind that although the board is the most important role-player in the strategy process, it is not the only one. Other participants in the organisation's strategic process include:

(i) Executive strategy team leader;

(ii) The CIO who will provide guidance and direction to the executive strategy team. These two entities are normally responsible for the formulation of the strategy;

(iii) Support team - This team is charged with amongst other things: "…managing the process; maintaining process documentation, providing expertise in methods; preparing "strawpersons" and drafts for strategy teams to review; coordinate meetings and read-outs, conducting quality control; coordinating education, and guiding and facilitating debate"; and

(iv) Other stakeholders for instance employees Boar (n 102) 297-299.

5.4.7 Barriers to strategic alignment success

Strategic alignment, similar to performance measurement is dependant on two critical success factors, namely (i) top management support and commitment; and (ii) effective communication and rewards and recognition. [149]

(i) **Acceptance**. To gain top management commitment and support is a huge barrier in the strategy process. [150] "Everyone salutes, but few march, and even fewer charge." [151] Without top management support and commitment these programs will not be taken seriously by lower levels of the organisation.

(ii) **Communication.** The strategy must be clearly communicated to all levels of the organisation. [152] A perfectly formulated strategy will be useless if it is not communicated to those people who are expected to execute it.

5.4.8 Strategic implications of information security [153]

The **objective of information security strategic alignment** is to develop an information security strategy that is "consistent with the competitive strategy of the organisation, focuses on a few important missions, and feasible given resources and constraints."[154]
The following framework is representative of information security strategic alignment in its most simplistic form:[155]

[149] Wade and Recardo *Corporate Performance Management* (2001) 50.
[150] (n 124) 207.
[151] ibid.
[152] ibid.
[153] For a step-by-step reference guide on how to achieve strategic alignment, consult Meador "IT / Strategy alignment" (last visited 9 September 2002) http://www.it-consultancy.com 6.
[154] Meador "IT / Strategy alignment" (last visited 9 September 2002) http://www.it-consultancy.com 5.
[155] For a comprehensive discussion on strategic alignment, specifically pertaining to information technology consult Annexure F.

Phase 1 "Where we need to go"

Objective of phase is the development of an information security strategy.[156]

(i) Assess current alignment between information security and competitive strategy and formulate the new information security strategy;

(ii) Identify the impact information security has on business strategy;

(iii) Draft information security strategy alternatives; and

(iv) Identify and refine the information security strategy.

Phase 2: "What we need to get there and when we need it"

Objective of this phase is to define strategic information security infrastructure "that will enhance and facilitate existing competitive strategies and potentially enable new strategic actions not previously envisioned."[157]

(i) Assess current information security environment;

(ii) Review current business processes; and

(iii) Design strategic information security infrastructure.

Phase 3: "How will we get there?"[158]

Objective of this phase is to set out practical steps to be followed to achieve alignment.

5.4.9 Conclusion

Organisations no longer have the choice of deciding if they want to align their organisational strategy with departmental strategies. If they wish to survive in the information age they will have to make a conscious effort to achieve strategic alignment, as alignment, much like information security,"…is mandatory; it is not optional…".[159]

[156] (n 154) 8.

[157] (n 154) 14.

[158] See Annexure G for an example of an "Alignment Checkup."

[159] (n 7) 4.

Organisations should however keep in mind that “strategy is not something the organisation does, but rather something it lives.”[160]

[160] (n 100) 190.

5.5 PART FOUR: THE BUSINESS CASE FOR INFORMATION SECURITY

Business drivers behind the increased importance of information security would include the following:

(1) "Compliance enforcer and advisor"[161]

Because of the fact that technology has elevated itself as a critical success factor, increased legal consideration is being given to technology and related matters.[162] Issues ranging from privacy, labour law, data protection, copyright, and specifically the protection of information as one of the most important assets of the organisation, have received considerable attention.[163] The USA as well as the European Union (EU) have enacted legislation, and issued directives dealing specifically with data security and protection.[164]

Benefit to top management: information security governance ensures that management complies with laws and regulations pertaining to issues relating to the protection of information.[165]

(2) "Business enabler and company differentiator"[166]

The information age demands of organisations to establish a presence on the Internet. Yet, one of the biggest concerns for customers and suppliers doing business on the

[161] (n 1) 245.

[162] ibid.

[163] ibid.

[164] In the United States of America legislation such as the US department of Health and Human Services rule, and the Gramm-Leach-Billey Act compel organisations to ensure data security and protection. The European Union (EU) issued a set of standards in 1998 that regulates the protection and exchange of personal information. It contains strict provisions when wanting to exchange information beyond the EU. For a comprehensive list of national and international information security legislation, regulations and standards, consult Annexure A.

[165] (n 1) 245.

[166] ibid.

Internet is security and trust.[167] Exemplary information security practices will enable the organisation to build a reputation for being a secure and trustworthy e-business. Therefor customers and suppliers alike will have the confidence to do business with the organisation.[168]

Benefit to top management: information security gives an organisation the competitive advantage by providing safe and secure services and/or products.[169]

(3) "Total quality management contributor"[170]

The organisation uses information to base its decisions on regarding the production of products and the delivery of services. The quality of services and/or products the organisation provides or delivers will emanate from the confidentiality, integrity and availability of this information.[171] A security incident or breach that materialises will result in halted business operations, loss of productivity and loss of revenue. More importantly a security incident or breach will do irreparable damage to the organisation's reputation, resulting in an all but complete loss of customer and shareholder confidence. Rebuilding trust in the organisation is a costly, onerous and near impossible task.[172]

Benefit to top management: delivery of high quality services or products, on time, and within budget.[173]

[167] ibid.
[168] ibid.
[169] ibid.
[170] ibid.
[171] ibid.
[172] Boespflug, Neal and Crowe "Secure your systems now: just one hacker can wreck your business" (last visited 18 April 2002) http://www.itweb.co.za 1.
[173] (n 1) 245.

(4) "Peopleware controller" [174]

Information security governance helps top management to manage one of the biggest, yet least acknowledged threats – the insider threat. [175] Internal threats continue to be one of the biggest threats facing organisations, whether the threat originates from a disgruntled employee or merely a negligent employee.

Benefit to top management: information security governance provides organisations with the infrastructure to manage internal threats through, amongst other things, policies, standards, procedures and guidelines. [176]

(5) "Strategic asset of the organisation"

"Information is a strategic asset. Therefor, information protection is a strategic requirement." [177] Organisations are beginning to realise and acknowledge the value of information as a mission critical business asset, consequently information security will leverage the value of information. [178]

5.6 Conclusion

Information security governance is concerned with mainly two issues: (i) that information security contributes value to the organisation, by not only supporting it, but also enabling it; and (ii) that information security risks are extenuated to an acceptable level. Often the board might find itself in a situation where "a commercially desirable action may appear in conflict with good governance principles."[179] For example the board might be

[174] ibid.
[175] ibid.
[176] (n 1) 246.
[177] (n 1) 244.
[178] Symantec "The value of information security" (last visited 18 May 2003) www.symantec.com 4.
[179] (n 106) 30.

contemplating cutting back or abolishing information security (safeguards) to save money. Although the intangible benefits attached to information security are difficult to place a monetary value on, information security forms "such an integral part of good governance that the balance should tilt in favour of its retention."[180]

Therefor it may be concluded that the elusive value of information security may be captured in two ways: (i) through a valuation methodology such as performance measurement, and specifically the balanced scorecard, that will indicate how information security contributes to the financial health of the organisation; and (ii) aligning investments in information security with the organisation's strategic objectives. Thereby enabling information security to function as a business supporter and enhancer. At present the value delivered by information security goes far beyond trimming costs and boosting productivity,[181] information security is transforming the very nature of business as we know it.[182]

The bottom line: information security will help organisations leverage competitive advantages, increase its overall effectiveness and productivity, and ensure that the organisation remains flexible enough to adapt to changes occurring within the business and technological environment. Ultimately information security governance makes good business sense.

This chapter aimed at convincing the board of directors and top management alike of the business value of information security governance, by capturing the illusive value of this discipline. However, before the organisation will be able to enjoy the numerous benefits promised by this discipline, they will have to overcome one final hurdle: the successful implementation of information security governance within the organisation. The next chapter will therefor provide directors and top management with a useable framework to guide in their efforts.

[180] ibid.

[181] Noyes "New orders of magnitude" (last visited 18 November 2002) http://www.cio.com/archive/020102/overview_content.html 1.

[182] (n 181) 1.