The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan

Maria Soto Corpuz
Information Security Institute, Queensland University of Technology
Brisbane, Queensland/4000, Australia

Extended Abstract

Keywords**: information security management, enterprise information security policy, strategic management**

1. INTRODUCTION

Information security has been recognized as a core requirement for corporate governance that is expected to facilitate not only the management of risks [1][2], but also as a corporate enabler that supports and contributes to the sustainability of organizational operations [3]. In implementing information security, the enterprise information security policy is the set of principles and strategies that guide the course of action for the security activities [4] and may be represented as a brief statement that defines program goals and sets information security and risk requirements [5].

The enterprise information security policy (alternatively referred to as security policy in this paper) that represents the meta-policy of information security [1] is an element of corporate ICT governance [6] and is derived from the strategic requirements for risk management and corporate governance. Consistent alignment between the security policy and the other corporate business policies and strategies has to be maintained if information security is to be implemented according to evolving business objectives. This alignment may be facilitated by managing security policy alongside other corporate business policies within the strategic management cycle.

There are however limitations in current approaches for developing and managing the security policy to facilitate consistent strategic alignment. This paper proposes a conceptual framework for security policy management by presenting propositions to positively affect security policy alignment with business policies and prescribing a security policy management approach that expounds on the propositions.

2. LIMITATIONS IN CURRENT APPROACHES

Organizational executive management often considers matters relating to information security to be mainly technical issues under the domain of information technology and commonly delegated to the IT department [5][6][7][8]. Observations by researchers [8][9] on current information security management system frameworks and standard practice guidelines [10][11][12][13] imply that these standards only provide suggestive definitions and characteristics of information security policy. There is a lack of definition of a process approach on its development and management. Information security management standards are checklists of security controls defined in generic terms [6]. Other security policy development and maintenance frameworks [14][15] that are proposed to address the limitations of the checklist approach relate to security activities that are usually conducted separately to those of corporate governance and risk management activities. Consequently, some security policy theories propose aligning the information security policy with the IT strategic planning [5][15]. In adopting these theories, full integrative relationship between security policy development and other strategic management activities such as strategic planning and corporate governance remains a challenge. The security policy is rendered as an IT-focused initiative with inadequate reference and at times misalignment with the other corporate strategic objectives that are not directly related to IT.

Further research on security policy approaches adopt the risk management framework for information security management systems as a security planning process [2][16] and as a full integrative management framework [17] between information security and corporate risk to present the actual linkages between security policy and corporate risk policy. However, these policy theories and approaches restrict the alignment positioning of information security policy with that of IT planning as it is seen as a technical concern [8][18] or at most with that of corporate risk planning as an operational risk [17].

The restrictive alignment positioning inhibits the relationship of the security policy (and consequently the management and implementation of information security) with other strategic policies and as a consequence does not encourage coordination between the different strategic policy domains. This perspective poses inherent disadvantages to the overall implementation of information security as the strategic alignment of the security policy with the other business policies is not manifested and therefore hardly understood at the board level. As shown in Figure 1, the security policy is excluded from the corporate strategic management cycle as a business policy and alignment to other corporate business policies such as the corporate governance policy is not directly accommodated.

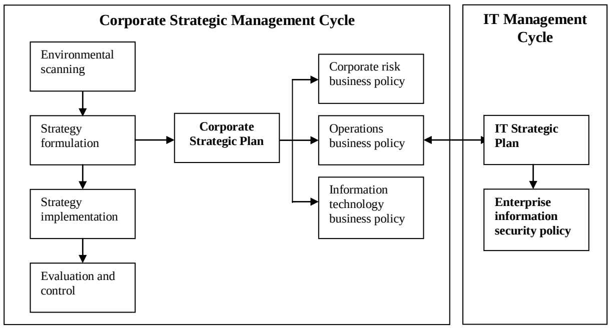
Corporate Strategic Management Cycle
IT Management Cycle
Environmental scanning
Strategy formulation
Strategy implementation
Evaluation and control
Corporate Strategic Plan
Corporate risk business policy
Operations business policy
Information technology business policy
IT Strategic Plan
Enterprise information security policy

Figure 1 Traditional Alignment Approach for Enterprise Information Security Policy

The resulting security policy usually consists of an unstructured checklist set of security controls that is developed without the in-depth understanding to substantiate the requirement for functionality and value of such security policy and controls. Lacking in the corporate alignment on the strategic level, the security policy is dropped out of scope as a corporate-level agenda item. A consequence of this issue is the difficulty in obtaining the required support at the executive level [19] resulting inadequate allocation of resources and corporate support required for successful delivery of information security outcomes.

The strategic management cycle is discussed in the following section to provide a brief background upon which to base the conceptual development of the proposed security policy framework.

3. STRATEGIC MANAGEMENT AND BUSINESS POLICY

Strategic management is defined as a set of managerial decisions and actions that determines the long-run performance of a corporation [20][21][22]. The basic model of strategic management consists of four major phases namely: (1) environmental scanning; (2) strategy formulation; (3) strategy implementation; and (4) evaluation and control [22][23][24]. The environmental scanning stage involves the identification of the internal and external strategic factors that may affect the future of the organization [22].

The second stage of strategy formulation involves the development of the long-range plan through the definition of the mission, objectives, strategies and policies [24]. The mission statement defines the purpose and existence of the organization while the statement of objectives identifies what needs to be accomplished and by when to achieve the mission statement. Based on the defined mission and objectives, strategies are then developed. A strategy lays out the plan to achieve the organization's mission and objectives and requires broad directives to guide the organization's strategy formulation with its implementation [24]. These broad directives are defined in a corporate business policy [21]. As an element of strategic management, the business policy is the general management of integrated internal functions to ensure that decision's and actions are aligned with and in support of the defined mission, objectives and strategies [22].

The third stage of the strategic management model is the strategy implementation. Strategy implementation consists of developing and implementing the programs, budgets and procedures necessary to action the strategies and policies defined in the strategy formulation stage [23]. The last stage is the evaluation and control stage which involves the process of monitoring the actual performance and comparing the results with that of the defined performance objectives as a condition of business improvement [24]. The strategic management model is adopted in the development and overall management of strategic business policy strategies and may be utilized for developing security policy as a strategic business policy.

4. CONCEPTUAL FRAMEWORK FOR ENTERPRISE INFORMATION SECURITY POLICY MANAGEMENT

In this section, propositions are formulated and presented followed by the security policy management approach that expounds on the propositions.

Security Policy as Corporate Business Policy

Corporate business policies are required to provide guidelines to ensure that all decisions and activities are aligned with the defined strategies as part of good corporate governance [22] [24]. As information security has become a crucial part of corporate governance [1][7] that focuses more on people, processes and information in addition to IT [2], the security policy that provides the critical direction-setting aspect of information security is one of the most important controls of corporate governance [9].

The security policy is based on business and organizational requirements to manage risks [3] and it is balanced against cost efficiencies and business benefits [10]. It requires continuous assessment and revision to address evolving risks [25][26]. The continuous assessment of security policy ensures practices and procedures within the security policy are coordinated and integrated [11].

Policy development for information security takes on concepts of strategic planning by way of objective setting and coming up with the program of projects to be undertaken according to the set business objectives. This apparent similarity where it is defined that the security policy contains a layered structure set of sub-policies and procedural implementation that need to be reviewed and assessed may be undertaken in the same manner as that of a corporate strategy or policy and its related program plan of business initiatives.

From this discussion, it may be considered that the development and management of the security policy is a strategic planning process derived from other corporate-level business policy requirements to ensure consistent alignment. The consistent alignment may be achieved by developing and managing the security policy as a business policy alongside the other strategic policies as depicted in Figure 2. This perspective addresses the limitations in current approaches that confines the alignment positioning of information security policy only to that of IT planning. The first proposition (P1) is presented as:

Proposition 1 (P1): *Developing security policy as a corporate-level business policy positively affects its consistent alignment with other business policies as part of corporate governance.*

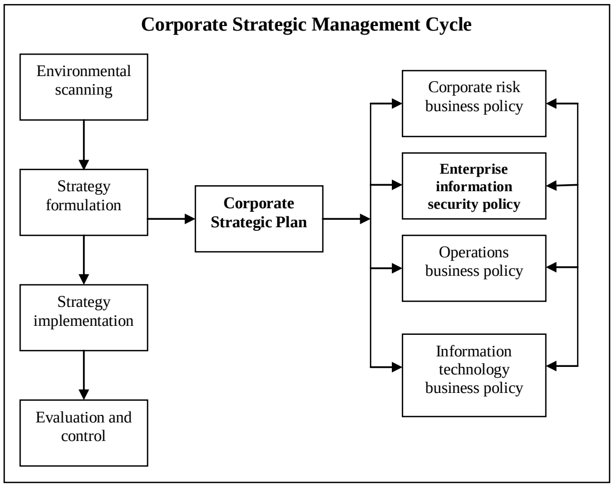
Corporate Strategic Management Cycle
Environmental scanning
Strategy formulation
Strategy implementation
Evaluation and control
Corporate Strategic Plan
Corporate risk business policy
Enterprise information security policy
Operations business policy
Information technology business policy

Figure 2 Proposed Alignment Approach for Security Policy as a Strategic Business Policy

Integrating Security Policy within the Strategic Planning Process for Alignment

Research studies on business planning (BP) and information systems planning (ISP) have presented various integration approaches [27][28][29][30] that may be utilized to address alignment issues across corporate functions. The need for aligning information systems planning with business planning have been demonstrated by prescriptive [27][29] and empirical studies [31][32][33] as contributing to the assurance that business objectives are met and effective information technology investments are made. Information systems planning should be integrated within business planning to achieve alignment through full integrated planning [34][35]. This involves developing both the BP and ISP strategies at the same time using the same planning process and establishing an integrative relationship between BP and ISP. The presence of the alignment mechanisms of content, timing and personnel inherent in a full integrative relationship [36] provides benefits to organizations as a result of improved coordination of information systems plans with business plans [31]. It has been asserted that information systems should not be regarded as separable from business strategy but instead fully integrated with the corporate policies [37]. As security policy development takes on the conceptual elements of information systems planning, the adoption of the full integrative planning approach between security policy and strategic business policies is applicable.

Strategizing information security as a business policy may be then be approached by integrating security policy development within the traditional strategic planning and management cycle. This approach provides for consistent coordination of changes in requirements between the security policy and the other corporate business policies as presented in Figure 3.

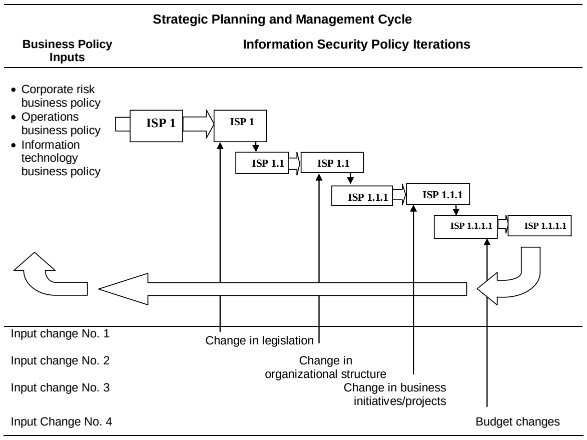
Strategic Planning and Management Cycle
Business Policy Inputs
Information Security Policy Iterations
• Corporate risk business policy
• Operations business policy
• Information technology business policy
ISP 1
ISP 1
ISP 1.1
ISP 1.1
ISP 1.1.1
ISP 1.1.1
ISP 1.1.1.1
ISP 1.1.1.1
Input change No. 1
Change in legislation
Input change No. 2
Change in organizational structure
Input change No. 3
Change in business initiatives/projects
Input Change No. 4
Budget changes

Figure 3 Timeline of Change Alignment within the Strategic Management Cycle

This manner of integrating different management domains by utilizing the same management framework process to enhance alignment has been prescribed for other corporate governance activities such as risk management [17]. From this perspective, the second proposition (P2) is formulated:

Proposition 2 (P2): *Integrating security policy development within the strategic planning and management process positively affects the consistent alignment between the business policies and the security policy.*

The Information Security Policy Management within the Strategic Management Cycle

The proposed approach for security policy management is developed by adopting the strategic management model to facilitate full integrative alignment as shown in Figure 4. This integrative approach depicts the security policy as a corporate business policy that is consistently aligned with business policies and objectives.

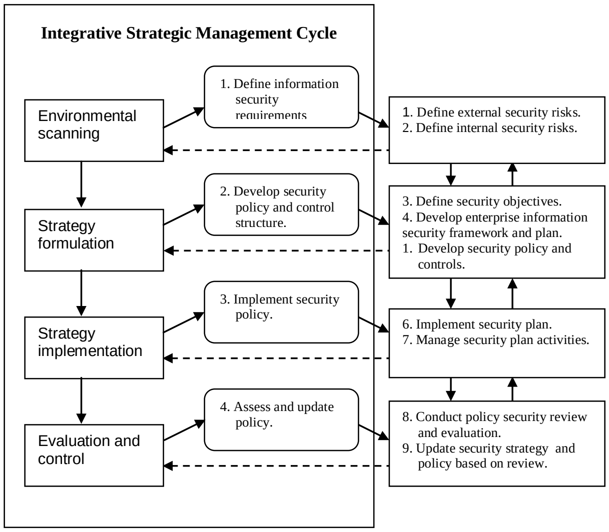
Integrative Strategic Management Cycle
Environmental scanning
Strategy formulation
Strategy implementation
Evaluation and control
1. Define information security requirements
2. Develop security policy and control structure.
3. Implement security policy.
4. Assess and update policy.
1. Define external security risks.
2. Define internal security risks.
3. Define security objectives.
4. Develop enterprise information security framework and plan.
1. Develop security policy and controls.
6. Implement security plan.
7. Manage security plan activities.
8. Conduct policy security review and evaluation.
9. Update security strategy and policy based on review.

Figure 4 Integrative Approach for Developing Enterprise Information Security Policy

Briefly, the proposed framework process is described as follows:

Step 1 ***Define enterprise information security requirements*** **(environmental scanning)** – Environmental scanning for strategic planning involves defining the external factors and the internal factors affecting the business environment in all aspects [22]. This step enables the organization to establish the key business process and prioritize the focus of the strategic management efforts. The SWOT (strengths-weaknesses-opportunities-threats) analysis [38], a tool used in strategic management and business policy development, can be employed in environmental scanning. For the security policy, this step accommodates the interplay and coordination of the various factors involved in developing each corporate strategy or policy with that of the security policy requirements on the strategic level. This approach expands the security policy requirements to include the risks involved in corporate governance, risk management and business operations in addition to the usual IT-related aspects of security risks. As an example, corporate governance risks that are not usually considered in traditional non-integrative approaches but are now identifiable in this step involve risks pertaining to staff misconduct and organizational disaster management. The output of this step is the Enterprise Information Security Risk Assessment Report.

Step 2 ***Develop security policy and control structure*** **(strategy formulation)** - The costs and trade-offs of the proposed enterprise information security policy and the corresponding policy control solutions as aligned to the other business policy control structures are determined in this activity. Detailed examples of controls that are developed based on the other business policy requirements such as risk management policy and operational business policies include security planning, processing authorization, incident response, configuration management, logical access control and secure application architecture. Useful techniques for evaluating risks and developing the strategies involve group decision-making employing the Delphi technique [39] and deriving decision trees to arrive at resolutions. For this step, the integrative approach allows the matching of costs and benefits between the security policy and control structures with those of the corporate business requirements on the strategic scale. The deliverable output of this process is the Enterprise Information Security Policy.

Step 3 ***Implement security policy*** **(strategy implementation)** - Based on the enterprise information security policy derived in Step 2, the enterprise information security plan is developed. The mitigating controls for the enterprise-wide security risks identified through the security risk assessment process incorporates strategic business initiatives and are finalized and drawn into a comprehensive enterprise information security policy set of initiatives or projects. The developed information security plan may take the form of a program of projects to implement the set of security controls which may be new treatments, additional controls or modifications to current controls. An important element of the security plan is the security architecture that consists of the security technologies as part of the implemented control structure of the security policy. One such example is the security policy stating a requirement for network security. The security technology that will meet this policy requirement may involve the deployment of an antivirus and firewall system. The output of this step is the Information Security Plan that details the projects and the taxonomy of procedural policies.

Step 4 ***Assess and update policy according to evolving business requirements*** **(evaluation and control)** - In this step, the review process for each policy development cycle is conducted to provide the basis for the next round of policy development activities. This activity fulfills the requirement for business improvement as required in strategic management. Coordinating and correlating lessons learned for the policy review process with that of the corporate business policy review activities, including that of corporate risk will further enhance future policy development activities as strategic objectives are met.

3 Conclusion

The goal of enterprise information security is to enable an organization to satisfy all of its strategic business objectives by implementing systems considering information technology-related risks to the organization, its business partners and clients. Although presented in various ways, the definition and characteristics for developing the strategic policy for enterprise information security remains consistent in that the security policy should outline the organization's program set of initiatives to ensure the security controls based on risk mitigation strategies are implemented to meet business objectives.

This paper presents a conceptual framework for security policy management by introducing propositions on how treating the security policy as a business policy may positively affect consistent alignment between the different strategic level policies. The proposed full integrative planning approach for the enterprise information security policy conceptually demonstrates that the security policy can be presented as a business policy within the strategic management cycle. As such, it is argued that the security policy can take on integrated strategic planning activities alongside other strategic business policies. This integrative approach is conceptually illustrated to foster an interactive relationship between security policy and other business policies to facilitate changes according to evolving requirements. The challenge that remains is the readiness of organizations to acknowledge the strategic value of treating the security policy as a business policy by adopting the proposed framework. The recommended future research includes the adoption of the proposed security policy framework to establish applicability and the development of an assessment model for both the framework and the security policy to validate the framework propositions and identify elements of value as well as areas for improvement.

6. References

[1] R. Baskerville and M. Siponen, "An Information Security Meta-Policy for Emergent Organizations", **Logistics Information Management**, Vol. 15 No.5/6, 2002, pp. 337-346.

[2] E. Humphreys, "Information Security Management Standards: Compliance, governance and risk management", **Information Security Technical Report**, Vol. 13, 2008, pp.247-255.

[3] Organization for Economic Co-operation and Development OECD, **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**, OECD , 2002.

[4] W. Caelli, **Information Security Handbook**. Macmillan Publishers Ltd, 1991.

[5] V. LeVeque, **Information Security A Strategic Approach**, John Wiley and Sons Ltd, 2006.

[6] M. Siponen, "Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned from Software Maturity Criteria", **Information Management and Computer Security Vol. 10 (5)**, 2002, pp. 210-224.

[7] B. von Solms and R. von Solms, The 10 deadly sins of information security management, **Computers and Security**, 2004, Vol. 23, pp. 371-376.

[8] D.F. Lohmeyer, J. McCrory and S. Poggreb, "Managing Information Security, **McKinsey Quarterly Special Edition**, 2002, pp 12-15.

[9] K. Hone and J.H.P. Eloff, "Information Security Policy – What Do International Information Security Standards Say", **Computers and Security**, Vol. 21, Issue 5, 2002, pp. 402-409.

[10] International Standards Organization ISO/IEC, **ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements**, International Standards Organization, 2005.

[11] M. Swanson and B. Guttman, **NIST Generally Accepted Principles and Practices for Securing Information Technology Systems Special Publication 800-14,** National Institute of Standards and Technology, 1996.

[12] J. Cazemier, P. Overbeek, L. Peters, **IT Infrastructure Library Best Practice for Security Management**. Office of Government Commerce, Crown Copyright, 1999.

[13] IT Governance Institute ITGI, COBIT 4.0 **Control Objectives Management Guidelines Maturity Models**, ITGI, 2005.

[14] J. Rees, S. Bandyopadhyay and E. Spafford, "PFIRES: A Policy Framework for Information Security", **Communications of the ACM,** Vol. 45. No. 7, 2003, pp. 101-106.

[15] N. F. Doherty and H. Fulford, “Aligning the Information Security Policy with the Strategic Information Systems Plan”, **Computers and Security** Vol. 25, 2006, pp. 55-63.

[16] D. Straub and R. Welke, “Coping with Systems risk: Security Planning Models for Management Decision Making”, **MIS Quarterly**, 22(4), 1998, pp. 441-469.

[17] M. Corpuz and P. Barnes, “Integrating Information Security Policy Management with Corporate Risk Management for Strategic Alignment”, **The 14th World Multi-Conference on Systems, Cybernetics and Informatics Proceedings**, Vol 4, 2010, pp.337-342.

[18] B. von Solms, “Corporate Governance and Information Security”, **Computers & Security**, 20(3), 2001, pp215-218.

[19] A. Kankanhalli, H. Teo, B. Tan and K. Wei, “An Integrative Study of Information Systems Security Effectiveness”, **International Journal of Information Management** (23), 2003, pp.139-154.

[20] S. Tilles, “How to Evaluate Corporate Strategy”, **Strategic Management: Harvard Business Review** (Ed: R. Hamermesh), USA: John Wiley & Sons Inc., 1983, pp. 77-96

[21] D. Harvey, **Business Policy and Management**, Ohio: Charles E. Merrill Pub., 1982.

[22] T. Wheelen and J. Hunger, **Strategic Management and Business Policy: Concepts and Cases**, New Jersey: Pearson Prentice and Hall Pub., 2008.

[23] E. Bowman, H. Singh and H. Thomas, “The Domain of Strategic Management: History and Evolution”, **Handbook of Strategy and Management** (Eds: A. Pettigrew, H Thomas and R. Whittington), London: Sage Pub., 2006, pp.31-51.

[24] J. Kay, P. McKiernan and D. Faulkner, “The History of Strategy and Some Thoughts About the Future”, **The Oxford Handbook of Strategy** (Eds: D. Faulkner and A. Campbell), Oxford: Oxford University Press, 2003, pp.27-52.

[25] Institute of Chartered Accountants ICA, **Internal Control: Guidance for Directors on the Combined Code**. Institute of Chartered Accountants (England and Wales), 1999.

[26] Information Systems Security Association (ISSA). **Generally Accepted Information Security Principles** *(GAISP V3.0),* 2004, ISSA.

[27] W. R. King, “Strategic Planning for Management Innformation Systems”, **MIS Quarterly**, Vol 2 (1), 1978, pp. 27-37.

[28] W. R. King and R. W. Zmud, “Managing Information Systems: Policy Planning, Strategic Planning and Operational Planning, **Proceedings of the Second International Conference on Information Systems**, Boston, 1981.

[29] N. Goldsmith, “Linking IT Planning to Business Strategy”, **Long Range Planning**, Vol. 24, No. 6, 1991, pp. 67-77.

[30] A.L. Lederer and V.Gardiner, “Strategic information systems planning: The Method/1 approach. **Information Systems Management**, Vol. 9(3), 1992, pp. 13-20.

[31] A. L. Lederer and A. L. Mendelow, “Coordination of Information Systems Plans with Business Plans”, **Journal of Management Information Systems**, Vol. 6. No. 2, 1989.

[32] T. S.H. Teo and W. R. King, “Assessing the impact of integrating business planning and IS planning”, **Information and Management**, Vol. 30, 1996, pp. 309-321.

[33] Y.E. Chan, R. Sabherwal and J.B. Thatcher, “Antecedents and Outcomes of Strategic IS Alignment: An Empirical Investigation”, **IEEE Transactions on Engineering Management**, Vol. 53, No. 1, 2006, pp.26-47.

[34] T. S.H. Teo and W. R. King, “Integration between Business Planning and Information Systems Planning: An evolutionary-Contingency Perspective”, **Journal of Management Information Systems**, Vol. 14, No. 1, 1997, pp. 185-214.

[35] W. R. Synott, **The Information Weapon: Winning Customers and Markets with Technology**, New York, John Wiley, 1987.

[36] J.K. Shank, E. G. Niblock and W. T. Sandalls Jr., “Balance Creativity and Practicality in formal planning”, **Harvard Business Review**, 51 (1), January/February 1973, pp. 87-95.

[37] T. Smaczny, “Is Alignment between Business and IT the Appropriate Paradigm to Manage IT in Today’s Organization?”, **Management Decision**, 39(10), pp. 797-802.

[38] M. Porter, **The Competitive Advantage**, The Free Press, New York, 1985.

[39] T. Merna, **Risk Management at Corporate, Strategic Business and Project Level. MPhil Thesis**, 2002, UMIST, Manchester.