SAIS 2013Proceedings Southern (SAIS)

5-18-2013

EVALUATING THE PERFORMANCE OF INFORMATION SECURITY: A BALANCED SCORECARD APPROACH

Basil J. Hamdan
Virginia State University, bhamdan@vsu.edu

EVALUATING THE PERFORMANCE OF INFORMATION SECURITY: A BALANCED SCORECARD APPROACH

Basil J. Hamdan
Virginia State University
bhamdan@vsu.edu

ABSTRACT

This paper, a research in progress, presents a balanced scorecard based framework for managing and evaluating the performance of information security in organizations. Acknowledging the multi-dimensionality of information security and the various value propositions of different constituents, we contend that for organizations to maximize the value of their information security effort, they should strike a balance between four information security capabilities pertaining to four perspectives: the financial, the customer, the internal processes, and the learning and growth perspectives. The proposed framework supplements the traditional financial perspective with three non-financial perspectives and thus accounts for the qualitative and intangible benefits of information security. Furthermore, it captures the technical and socio-organizational dimensions of information security. Finally, the proposed framework, through its robust theoretical and methodological foundation, holds the promise of maximizing the effectiveness of the information security endeavor in organizations.

Keywords

Information security, balanced scorecard, performance evaluation

INTRODUCTION

As organizations become more reliant on information technologies and the Internet, their exposure to information security breaches will increase. Given the severity of the business impact that security breaches may have (e.g. lost revenues, lost productivity, customer dissatisfaction, legal fines, etc.), it comes as no surprise that information security has consistently ranked amongst the top 10 issues that concern IT professionals and scholars alike (Luftmann et al. 2008). In fact, it is this grave concern over the security of information systems and its critical impact on the viability of businesses that gave rise to a plethora of frameworks for information security, both in practice (e.g. the ISO/IEC 27000-series, the NIST Risk Management Framework, and the COBIT Model) and academia (e.g. Da Veiga et al. 2007; Eloff et al. 2005; Zuccato 2007).

Despite the proliferation of information security management frameworks, there is a lack of understanding about evaluating the performance of information security in organizations. This can be attributed to three reasons. First, many of the existing frameworks don’t provide inclusive mechanisms for evaluating their very performance. Second, limited independent research has been conducted to empirically evaluate the performance of information security under the current frameworks. Third, and most importantly, the information security field is yet to see a serious research effort aimed at developing theoretically-grounded and empirically-validated frameworks for evaluating the effectiveness of the organizational information security endeavor. In fact, it’s not an overstatement that there currently exists not a single holistic and dynamic framework that organizations can use to evaluate the performance of their overall information security effort. The current research purports to fill the gap by proposing a balanced scorecard framework for evaluating the performance of information security. The rationale behind choosing the balanced scorecard is twofold. First, the balanced scorecard as both a strategic management framework and a performance evaluation framework has been tried and proven effective. Second, the structure of the balanced scorecard makes it well-suited to capture the technical and socio-organizational dimensions of information security.

BACKGROUND

In this section, we examine the information security literature to describe the underlying perspectives and dimensions that may contribute to the formation of an evaluative framework of information security performance. Two issues pertinent to information security are delineated. The first issue tackles the ***what*** question (i.e. the unit of analysis) whereas the second issues tackles the ***how*** question (i.e. the evaluation approach).

The unit of analysis question is concerned with what should be involved in the management of information security and the subsequent evaluation of information security performance. A review of the information security research and practice reveals two major paradigms that have tackled the ***what*** question: the technical paradigm, which was dominant until early 1990’s and the socio-technical paradigm, which emerged in the mid 1990’s and remains the most prominent paradigm to date. As the name implies, the technical paradigm embraced a technical conceptualization of information systems and thus viewed information security as a technical issue best left to technicians. However, empirical evidence shows that technical controls *per se* are highly unlikely to be effective in securing the information systems as they leave the systems wide open to threats that they are not suited to mitigate. For example, access controls may prove very effective in preventing unauthorized users from accessing the systems but these very controls fail to prevent legitimate system users from causing adverse events by the means of human error, lack of security training, poor security awareness, etc.

Recognizing the shortcoming of the technical-based management of information security, many studies within the information security area (e.g. Da Veiga et al. 2007; Dhillon et al. 2001a; Trompeter et al. 2001; von Solms 2001) have broken away from the technical perspective towards a socio-organizational perspective which gave rise to the socio-technical paradigm. According to this paradigm, if information security is to be managed effectively, it is imperative that the emphasis goes beyond the technical controls to incorporate the managerial and organizational issues that may influence information security. Examples of such issues include, but are not limited to, the business value of information security, the regulatory compliance, the stakeholders' expectations, the internal business processes, the information security policies and procedures, and the roles and responsibilities of the various agents who influence or are influenced by information security. Today, a consensus is building among information security researchers that information security management is a multi-dimensional endeavor and that all dimensions must work together to create a secure information systems environment (von Solms 2001; Zuccato 2007). Consistent with the socio-organizational perspective, we argue that any effort aiming at evaluating the effectiveness of information security must move beyond evaluating the information security of the technical subsystem to include evaluating the information security as it pertains to the socio-organizational subsystem as well.

The evaluation approach question is concerned with how the evaluation should be carried out. A review of the information security literature reveals a skewed inclination towards quantitative evaluation techniques such as cost-benefit analysis, risk analysis, business impact analysis, and annual loss expectancy analysis (e.g. Cavusoglu et al. 2004; Gordon et al. 2002; Hoo 2002). For the most part, these quantitative models aim to quantify the magnitudes of losses resulting from information security breaches, the benefits resulting of information security solutions, and the return on information security investments with the ultimate goal of providing business justification of information security investments. In this research, we argue that the effectiveness of information security management cannot be reduced to simple financial or other quantitative measures as such measures capture only those benefits that are tangible or can be quantified when most of information security benefits are invisible or of less tangible nature at best. Therefore, we contend that quantitative evaluation models are necessary but not sufficient and that any effort aiming at evaluating the effectiveness of information security management should move beyond these models to consider the qualitative benefits of information security as well.

A BALANCED SCORECARD FOR INFORMATION SECURITY

In this research, we propose a balanced scorecard approach for evaluating the effectiveness of information security. Kaplan and Norton (1992) developed the Balanced Scorecard as a framework for strategic management and performance measurement. The framework organizes strategic objectives into four perspectives across which balancing is to be achieved: (1) the financial perspective (the strategy for growth, profitability, and risk viewed from the perspective of the shareholder), (2) the customer perspective (the strategy for creating value propositions from the perspective of the customer), (3) the internal business process perspective (the strategy for identifying, developing and maintaining business processes that create and deliver customer value and business value for shareholder), and (4) the learning and growth perspective (the strategy for creating a climate that supports organizational change, learning, innovation, and growth). In essence, the balanced scorecard complements the traditional financial perspective with three non-financial perspectives (customer, internal business processes, and growth and learning perspectives).

Drawing on the logic behind the balanced scorecard, we argue that for organizations to maximize the value of their information security effort, they should strike a balance between four interrelated strategic information security capabilities pertaining to the four perspectives of the balanced scorecard: (a) the capability to provide business value from information security investments in the form of better return on information security investments, higher productivity, and increased sales to name a few (hence, the financial perspective), (b) the capability to maximize the value of the internal customers (e.g. management, and employees) and external customers (e.g. regulators, external auditors, and customers) by supplying information security services and controls that match their demand and meet their value propositions and objectives (hence, the customer perspective), (c) the capability to identify the business processes an organization must excel at in order to fulfill its shareholders and other stakeholders' expectations (hence, the internal business processes perspective) and (d) the capability to create an information security conscious culture along with continuous learning which enable organizations to identify areas for improvement and to modify their strategies accordingly (hence, the learning and growth perspective). The following discussion delineates the four areas of the balanced scorecard from an information security perspective.

Financial Perspective

From a strict financial standpoint, the decision to implement a certain information security solution is contingent on whether or not the intended solution generates benefits surpassing the cost of installing and maintaining it. In this research we argue that the effectiveness of information security cannot be reduced to simple financial measures as obtained via quantitative evaluation techniques. This is because information security benefits are, for the most part, soft and intangible and thus cannot be expressed monetarily. For instance, an organization can spend $5,000 on a security awareness program but it is impossible to attach a dollar value to the achieved level of information security awareness or the productivity that would have been lost had an information security incident occurred due to a lack of security awareness.

Therefore, we contend that the financial perspective is necessary but not sufficient. The inherited deficiencies of the financial measures make them implausible for evaluating the effectiveness of the information security endeavor. Organizations which limit their evaluation to such measures are less likely to get the full picture which may cause them to be less inclined to support or to insufficiently invest in information security. Such unsupportive attitude will almost certainly weaken the effectiveness of the security program exposing the systems and the business to serious risks. Therefore, we contend that any effort aiming at measuring the performance of information security should move beyond the traditional financial metrics to consider a balance between the various perspectives of the information security.

Customer Perspective

In the previous financial perspective, we argued that organizations should consider other perspectives when managing and subsequently evaluating the effectiveness of their information security effort. One such perspective is the customer perspective which is concerned with the people who influence or are influenced by information security. More specifically, this perspective is concerned with the capability of the information security endeavor to maximize the value of customers by supplying information security services and solutions that meet their value propositions and expectations.

Unlike shareholders' values which are captured by the financial perspective, the values of other constituents (e.g. employees, customers, and regulators) are more subjective and less monetarily-based. The soft nature of these values adds to the complexity of evaluating the effectiveness of the information security as it necessitates the need for developing measures capable of capturing the gist of these values. This complexity is further intensified by the fact that each group of constituents has different set of values, needs, and behaviors with respect to the various information security issues surrounding them. For example, while employees are more concerned with having reliable and timely information at their disposal, customers are more concerned with protecting their privacy whereas regulators are more concerned with legal compliance. Therefore, the effectiveness of information security is largely dependent on the extent to which these values are understood and met.

Despite the unequivocal importance of understanding the various value propositions of various stakeholders to achieving effective information security, it is until very recently that information security research has taken on a serious effort to identify these values. Unsurprisingly, much of this effort has focused on the value propositions of employees; most likely on the ground that most security breaches are due to violations of safeguards by trusted personnel (Dhillon et al. 2001b). The following are examples of information security value propositions as espoused by various constituent groups: managing regulatory compliance (regulators), providing clear and reliable disclosures (boards of directors, external auditors), maximizing users' privacy (customers), managing systems availability (customers, employees), managing internal controls (external auditors), and providing reliable and timely information (employees, internal auditors). While it is critical for organizations to sufficiently and accurately identify the various value propositions, it is also important to identify and institutionalize the processes necessary to achieve these propositions. Hence, the internal processes perspective.

Internal Processes Perspective

The internal process perspective is concerned with identifying the internal processes that an organization must excel at in order to fulfill its shareholders and other stakeholders' expectations. Failure to identify the right processes may result in processes that have little, if any, to do with the stakeholders' values leading to ineffective information security. Therefore, it is of paramount importance that organizations identity the right kind of internal processes. Once these processes are determined, organizations can then gear their information security effort to supply information security services and products that match the demand of the various stakeholders.

Within the realm of information security, both research-based literature and practitioner-based publications offer a host of processes that are presumably essential for sound information security management. Examples of such processes include, but are not limited to, access control management, identification and authentication management, information security policy creation and enforcement, regulatory compliance management, and business continuity management (Ma et al. 2008). Interestingly, each of these processes can be mapped to a value proposition from the customer perspective. For instance, the business process of ensuring regulatory compliance is directed at regulators, the business process of ensuring privacy and systems availability is directed at customers, the business processes of creating security conscious culture and defining roles and responsibilities are directed at employees.

Learning and Growth Perspective

The learning and growth perspective is concerned with the future readiness of the information security effort. More specifically, it is concerned with ensuring the organizational capability to not simply execute the current internal business processes and achieve the current value propositions but also to predicatively and proactively adapt to changes in the business, IT, and security environments. We therefore argue that for organizations to triumph in managing information security, it is of utmost importance that they do not merely rely on static strategies or objectives for information security. Instead, strategies should be continuously revised, by adding new value propositions and business processes and/or modifying existing ones, to reflect the dynamic nature of business environment and the new security challenges.

Drawing upon the information security literature (e.g. Dhillon et al. 2006; Trompeter et al. 2001; von Solms 2001), we posit that the future readiness is based on five major capabilities whose importance varies from an organizational context to another: (1) the capability to create and promote a security conscious organizational culture through security training and awareness as well as policy enforcement, (2) the capability to attract and retain skilled and knowledgeable employees, especially information security specialists, in order to prepare for potential changes and challenges, (3) the capability to create an ethical organizational climate by building trust and a system of rewards , (4) the capability to provide innovative information security services and controls capable of mitigating the new threats , and (5) the capability to attain a real-time and double-loop learning. Put together, these abilities will enable the organizations to continuously identify areas for improvement and modify their information security strategies accordingly.

Table 1 below summarizes the four perspectives of the proposed balanced scorecard from information security point of view.

<table>
<tr><th rowspan="2">Financial Perspective</th><th colspan="7">Objectives</th></tr>
<tr><td colspan="2">Higher shareholder value</td><td colspan="2">Higher Sales</td><td colspan="3">Higher Productivity</td></tr>
<tr><th rowspan="4">Customer Perspective</th><th colspan="4">External Constituents</th><th colspan="3">Internal Constituents</th></tr>
<tr><th>Regulators</th><th>Board</th><th>Customers</th><th>External Auditors</th><th>Management</th><th>Employees</th><th>Internal Auditors</th></tr>
<tr><td rowspan="2">Manage regulatory compliance</td><td rowspan="2">Provide reliable disclosures</td><td>Manage privacy</td><td>Manage internal controls</td><td>Manage security risk</td><td>Manage availability</td><td rowspan="2">Manage internal controls</td></tr>
<tr><td>Manage availability</td><td>Provide reliable disclosures</td><td>Provide reliable disclosures</td><td>Provide reliable data</td></tr>
<tr><th rowspan="5">Internal Processes Perspective</th><th colspan="7">Processes</th></tr>
<tr><td>Ensuring Regulatory Compliance</td><td>Providing effective reporting</td><td>Ensuring privacy</td><td>Managing external IT audit</td><td>Creating security policies & compliance</td><td>Managing access control</td><td>Managing internal IT audit</td></tr>
<tr><td colspan="2" rowspan="3"></td><td>Ensuring availability</td><td rowspan="3"></td><td>Defining roles & responsibilities</td><td>Managing identification</td><td rowspan="3"></td></tr>
<tr><td>Ensuring Integrity</td><td>Developing security programs</td><td>Managing authentication</td></tr>
<tr><td></td><td>Creating contingency plans</td><td></td></tr>
<tr><th rowspan="2">Learning & Growth Perspective</th><th colspan="7">Capabilities</th></tr>
<tr><td colspan="2">Attract & retain skilled employees</td><td>Promote Ethical climate</td><td colspan="2">Create & promote security conscious culture</td><td>Double loop learning</td><td>Innovation</td></tr>
</table>

Table 1: A Balanced Scorecard for Evaluating Information Security Performance

So far, we discussed the four perspectives of the proposed balanced scorecard from an information security point of view with examples on each perspective. We briefly discuss how the balanced scorecard helps managers in linking information security strategies, long term in nature, with short-term actions. Specifically, we argue that lofty information security strategic objectives such as achieving higher productivity, maximizing information security, and managing regulatory compliance cannot be translated into actions if there is no or little understanding of how the actions of the various constituents could or could not contribute to their realization. For them to be understandable and thus potentially executable, information security strategies must first be expressed in terms of an integrated set of information security objectives and measures for the four perspectives of the balanced scorecard. These objectives are determined by the constituents who would realize the security vision and those have vested interest in its realization. Once the objectives and measures are determined, managers must determine the set of actions and activities (i.e. performance drivers) that will drive them towards achieving the specified objectives.

Table 2 below illustrates the utility of the balanced scorecard in linking the short-term actions with the strategic objectives for information security.

Perspective		Objectives	Measures	Performance Drivers
Shareholders		Enhancing productivity	% Change in productivity rate	Systems availability Employees satisfaction
		Increasing sales	% Change in sales	Customers and employees satisfaction
Customers	Customers	Ensuring privacy	The number of privacy complaints	Imposing rules against disclosure of customer information
	Employees	Ensuring the availability of the systems	The average downtime of the systems	Installing intrusion prevention systems Creating regular back ups
Internal Business Processes		Enhancing security policy compliance	Number of incidents of regulatory incompliance Level of regulatory compliance understanding	Developing an understanding of legalities and regulations
Growth and Learning		Developing and maintaining and ethical environment	Level of employees' morale	Building trust Implementing a performance based incentive system

Table 2: A Balanced Scorecard for Linking Short-term Objectives to Strategic Objectives

CONCLUSION

Information security management is a multidimensional-resource allocation process. As such, organizations should strike a balance while crafting and carrying information security strategies. Such balance would be easier to achieve, manage and evaluate if based on a comprehensive and standardized framework. One such framework is the Balanced Scorecard. The current research proposes and develops a balanced scorecard for information security to evaluate the effectiveness of information security from four different perspectives: the financial perspective (shareholder's view), the internal business process perspective (process based view), the customer perspective (value-adding view), and the learning and growth perspective (future view).

This research is still in an early stage. We plan to scan the literature to create a comprehensive list of information security objectives. Next, we plan to develop performance measures and to identify performance drivers to link the strategic objectives with the short term actions. A long term objective of this research is to develop an inclusive information security management profile that renders high levels of effectiveness across the various perspectives of the information security balanced scorecard. The ultimate goal is to develop an information security management theory that explains and predicts the effectiveness of the information security practice.

In the end, it is our hope that the discussion and ideas presented in this paper will simulate interest and research on information security performance evaluation.

REFERENCES

Cavusoglu, H., Mishra, B., and Raghunathan, S. "A model for evaluating IT security investments," *Commun. ACM* (47:7) 2004, pp 87-92.

Da Veiga, A., and Eloff, J. H. P. "An Information Security Governance Framework," *Information Systems Management* (24:4), Fall2007 2007, pp 361-372.

Dhillon, G., and Backhouse, J. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* (11:2) 2001a, p 127.

Dhillon, G., and Moores, S. "Computer crimes: theorizing about the enemy within," *Computers & Security* (20:8) 2001b, pp 715-723.

Dhillon, G., and Torkzadeh, G. "Value-focused assessment of information system security in organizations," *Information Systems Journal* (16:3) 2006, pp 293-314.

Eloff, J. H. P., and Eloff, M. M. "Information security architecture," *Computer Fraud & Security* (2005:11) 2005, pp 10-16.

Gordon, L. A., and Loeb, M. P. "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.* (5:4) 2002, pp 438-457.

Hoo, K. J. S. "How much is enough? A risk-management approach to computer security," Stanford University, 2002, pp. 16-17.

Kaplan, R. S., and Norton, D. P. "The Balanced Scorecard--Measures That Drive Performance," *Harvard Business Review* (70:1) 1992, pp 71-79.

Luftmann, J., and Kempaiah, R. "KEY ISSUES FOR IT EXECUTIVES 2007," *MIS Quarterly Executive* (7:2) 2008, pp 99-112.

Ma, Q., Johnston, A. C., and Pearson, J. M. "Information security management objectives and practices: a parsimonious framework," *Information Management & Computer Security* (16:3) 2008, pp 251-270.

Trompeter, C. M., and Eloff, J. H. P. "A Framework for the Implementation of Socio-ethical Controls in Information Security," *Computers & Security* (20:5) 2001, pp 384-391.

von Solms, B. "Information Security -- A Multidimensional Discipline," *Computers & Security* (20:6) 2001, pp 504-508.

Zuccato, A. "Holistic security management framework applied in electronic commerce," *Computers & Security* (26:3) 2007, pp 256-265.