2008

Information security governance and Boards of directors: Are they compatible?

Endre Bihari
Swinburne University

DOI: 10.4225/75/57b5595fb8768
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2008.

Information security governance and Boards of directors: Are they compatible?

Endre Bihari
Swinburne University
ebihari@swin.edu.au

Abstract

This paper presents a critique of emergent views on the roles of the boards of directors in relation to information security. The analysis highlights several concerns about the separation and validation of proper theory and business assertions of information security at board level. New requirements articulated by industry bodies – represented by a selected group of experts and evident in literature – are compared to the underlying theory of corporate governance to identify possible discrepancies. The discussion shows in particular the importance of staying within the theoretical underpinnings of corporate governance when discussing the topic of governance in general and in relation to boards of directors' responsibilities. Our critique opens up more opportunities to clarify information security's role and relationship to corporate governance. We seek to draw particular attention to the appropriate separation of governance and management. This latter point we hope will encourage academics and business practitioners to reflect on current corporate and individual biases and on the way terms such as information security governance are represented.

Keywords

Corporate governance, information security, IT governance, board of directors, agency theory

Introduction

The scandalous corporate collapses in the early part of this decade necessitated a renewed emphasis on corporate governance. Accordingly, attention has been paid to corporate governance across all sectors and industries and at all levels of organisations. Legislative (Sarbanes-Oxley Act, CLERP9), government and industry regulatory (ASX 2003, SEC, NYSE, NASDAQ) and self-regulatory (AS 8000 series) requirements have all aimed to improve corporate governance practices.

A great number of these requirements targeted the boards of directors. This is not surprising as boards have significant responsibilities and perform essential and important functions governing the organisation. It is interesting to note that a number of industry groups have started to call for the establishment of IT and of information security governance (IIA, 2000, BSA, 2003 and CGTF Report, 2004, CIMA 2004, CICA, 2004) as part of the boards' activities and responsibilities. Some stated directly that information security was the responsibility of the board (ISACA 2001, Westby, 2004). Following these "call to action" documents, there have been attempts to redefine corporate governance (Hamaker 2003a and 2003b) by at least one organisation (ISACA). Although there seems to be a lack of theoretical foundation for such statements and definitions, the terminology (i.e. enterprise governance in place of corporate governance) has proliferated within the audit industry, causing confusion.

The question then arises as to whether those calls are justified and whether these calls are targeting the right level, i.e. the board? Should IT and/or information security be governed by the board? If yes, why and how, if not, who should be responsible for information security and at what level? Is corporate governance really changing as described and advocated? What is the underlying theory of IT and/or information security "governance"? Is this a legitimate terminology? Is there a legitimate theory? How is information security related to corporate governance?

Such questions prompted this study. Although these are all crucial issues with regards to the concept of information security's role in corporate governance, this paper focuses only on certain aspects of concerns raised. The intention was to ascertain the validity of claims such as "*information security should become an important and integral part of IT governance*" (ITGI 1, 2001); that "*IT governance is the responsibility of the board of directors*" (ITGI 2, 2003) and that "*the road to information security goes through corporate governance*" (CGTF 2004). Other, related issues indicated above will be discussed elsewhere.

Arguably, since boards of directors are often the subjects of such claims, the theoretical underpinnings for the boards' activities need to be looked at. The fundamental aspects of the boards' activities and how these activities fit into corporate governance need to be investigated. Drawing on the theoretical foundations of corporate governance, analyses could be made as to whether the aforementioned claims fit into the activities of the boards

of directors. A discussion on corporate governance and its theoretical underpinnings is presented in the following section in order to highlight the theoretical lens through which the research was conducted.

CORPORATE GOVERNANCE

The corporation is the paramount form of the business organisation. Similarly, corporate governance and the need for it is an integral part of the corporation itself. The most important pre-existing conditions for the corporation are democracy and private property (Bernstein, 2004). Protecting investors' private property while attracting them to invest their capital in the corporation is the fundamental goal of corporate governance (Berle and Means, 1932).

The essence of corporate governance can be derived from the belief that there are "*certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness*" as expressed in the American Declaration of Independence (1776). Corporate governance is meant to protect the individual's right of freedom in the market, by ensuring the moral behaviour of those acting in the marketplace (Smith, 1759). Interestingly, Smith later built his market theory and system of market capitalism on these principles (Smith, 1776).

These principles can be further understood in the context of the religious orientation of both the signatories of the Declaration of Independence and Smith. Millstein calls this the Micah principle (Millstein, 2004). It is derived from Micah 6:6-8 and advocates in effect fulfilling the spirit of the law rather than adhering only to the letter of the law. The concept in Micah 6:8 of "*to do justice, to love kindness*" (NASB) is seen to correspond with Smith's "*prudence, justice and beneficence*" and indicates an ethics that doesn't aim to deliberately cause damage to others while pursuing self-interest. This ethical stance is similar to Benjamin Franklin's *deist ethics* or what Weber calls the "protestant ethic" (Weber, 1930). Millstein argues therefore that "box-ticking" lacks substance and protecting shareholders' interests should be ingrained in the culture of boards (Millstein, 2004, p. 12) instead of being viewed as a set of rules that need to be conformed to.

In summary, the three core concepts of corporate governance are:

1. The inalienable rights of the individual;
2. The protection of these rights of the individual in the market;
3. The highly ethical behaviour of the actors in the market.

These three principles, especially the expectations of ethical behaviour, are at the core of most theories developed during the last 100 years. It can be argued that such an ethic and expression of virtue expressed by Smith and his contemporaries has somewhat disappeared in the ensuing decades leaving a vacuum, which many of the theories in corporate governance seem to be attempting to address. The principle of ethical behaviour advocated by Smith is still relevant today and it is therefore suggested that each theory be considered through the lenses of the above three principles. The theory that appears to fulfil those principles best is then suggested to be taken as the platform on which the industry body claims are going to be evaluated.

As the corporation and the marketplace itself became more complex, a number of – often competing – theories were developed to address such complexities:

- Agency theory deals with the issue of protecting shareholders' interests (Berle and Means, 1932). This is especially important when conflict between managers and shareholders (Jensen and Meckling, 1976, Jensen and Ruback, 1983) arises due to information asymmetry. This can be seen when self interest, coupled with insider knowledge, causes managers not to act in the interest of stakeholders.
- Resource Dependence Theory emphasises the relationship between the corporation and its environment (Pfeffer, 1982, Hayward and Boeker, 1998). The board is viewed as a tool "*to manage environmental uncertainty*" (Boyd, 1990). This theory appears to consider corporate governance within the field of finance (Shleifer and Vishny, 1997). This however seems to be a narrow view and it can be argued that many aspects of board activities can't be explained through finance, economics or accounting.
- Transaction Cost Economics argues that "transaction is the basic unit of economic analysis" (Williamson, 1981), and as such transaction needs to be matched with governance structure to enjoy better efficiencies (Williamson, 1979). The organisational behaviour approach this theory builds on provides interesting insights into board behaviour (Fama and Jensen, 1983), financing structures and ownership (Jensen and Meckling, 1976). The theory however doesn't seem to cover all three underlying principles discussed above.
- Stewardship Theory advocates that instead of the separation of board and managers, the combination of these two groups will service the shareholders' interest best (Donaldson, 1990, Donaldson and Davis, 1991, Davis, Schoorman and Donaldson, 1977). Yet this theory seems to focus more on the relationship between the two groups rather than on the tasks these groups perform (Albanese et al, 1997). While this study is interested in the relationship between governance and management, this theory seems to provide too narrow a lens for the investigation.
- Stakeholder Theory expands the theory of control beyond the shareholders and their agents (Davis et al, 1977, Freeman, 1984, Mitchell et al, 1977, Byrson, 2004). Everybody who has a legitimate interest in the enterprise or is affected by it has the right to influence the corporation (Donaldson and Preston, 1995). This view however equals the interests of participants (whether interested in or affected by the

corporation) and "*rejects the idea that the enterprise exists to serve the interest of its owners*" (Weiss, 1995). While it is acknowledged that a corporation can not operate in a vacuum with only its owners' best interests in mind, the necessary conditions that must be met can't replace completely the owners' interest. Such conditions include social and environmental responsibilities. Notwithstanding this macro environment, this theory seems to be more appropriate to public administration (Bryson et al, 2002) than to private enterprise.

From the above précis, it can be concluded that these theories address the three underlying concepts (individual's rights, market and ethical behaviour) to a certain degree. It could be argued however, that most of the aforementioned theories seem to miss at least one of the core concepts, thus providing an incomplete picture. Of the theories outlined above, it would appear that agency theory is the most successful in addressing all three concepts. In effect, the theory could be used to explain how corporations were governed. Furthermore, particularly in the context of corporate governance, there seems to be a renewed focus on agency theory (Colley et al, 2003) lately. The essence of the theory is also recognised in such cornerstone documents as the Cadbury (1992) or Dey (2004) Reports; in current legislations (Sarbanes-Oxley Act, 2002) or in current textbooks (Monks, 2001, Chew & Gillan, 2005). In order to clarify the connection between the agency theory and corporate governance (as well as the aspects of information security as part of corporate governance), the following section will explore the issue of corporate governance from an agency theory perspective.

AGENCY THEORY, CORPORATE GOVERNANCE, AND INFORMATION SECURITY

Agency theory advocates the separation of ownership and control of the corporation (Berle and Means, 1932). The key participants according to this theory are the principals (shareholders) and their agents. The principals delegate work to the agents who perform the work on behalf of the principals. A conflict arises when the interest or goals of the principals differ from their agents or their attitude towards risk differs. These two issues are known as "*the agency problem*" and "*risk sharing problem*" both of which agency theory attempts to solve (Eisenhardt, 1989).

Although the study of corporate governance today goes beyond the framework of Berle and Means, with considerable revision and refining comments (Monsen et al., 1968, Larner, 1970, Fama and Jensen, 1983 and perhaps most importantly, Zeitlin, 1974), it has set the terms of the debate on corporate governance for almost a century. It is important to note here, that the idea was not of Berle and Means' own devising, as Smith had drawn attention to the same issue in the late eighteenth century (Smith, 1776, p. 192).

As the divergence of interest between ownership and control (Berle and Means, 1968, pp.112) was identified, this separation gave birth to the professional management class (Cochran and Wartick, 1988), which later evolved into two distinct directions: management and governance (Taylor, 2002, Bhagat and Jefferis, 2005).

The distinction between management and governance has been defined along the lines of strategic direction setting and hands-on, operational activities (Mueller, 1979, Tricker, 1997).

> *Governance is concerned with the intrinsic, purpose, integrity and identity of the institution, with a primary focus on the entity's relevance, continuity, and fiduciary aspects. Governance involves monitoring and overseeing strategic direction, socio-economic and cultural context, externalities, and constituencies of the institution*. (Mueller, 1981, p.9)

The operational activities of management are not replicated at board level. As the agency theory that brought governance into focus indicates, there is a distance between the directors, the shareholders they represent and the managers they oversee. Governance ensures that the right managers are doing the right job in the right way, in the best long-term interest of the shareholders.

> *The governance role is not concerned with running the business per se, but giving overall direction to the enterprise* (Tricker, 1984, p.6.).

The separation of governance and management is also important from the viewpoint of who is in charge (Firstenberg and Mankiel, 1994 and Lorsch and McIver, 1989). The issue of controlling the corporation and the structure of relationships at the top is very important, because of the power and impact of the corporation (Berle and Means, 1932). As Lorsch and McIver presented, directors do not view themselves as pawns of management (Lorsch and McIver, 1989), but rather as managers of managers. However this "management" is different from the senior and middle manager activities and it is appropriate to use governance to describe the activities of the board of directors.

> *Management on the other hand, is more of a hands-on activity. In its traditional sense, management can be characterized as conducting or supervising action with the judicious use of means to accomplish certain ends. Management primarily focuses on specific goal attainment*

> *over a definite time frame and in a prescribed organization. Planning, staffing, administration and direction, measurement, control, innovation, representation, decision making, and operations are classical elements of management, which essentially strives to function as a closed, command and control system.* (Mueller, 1981, p.9)

Understanding the "management of management" concept of corporate governance is an essential element of contextualising terms like "IT governance" and "information security governance". Information security literature also suggests that there is a governance side and a management side (Posthumus and von Solms, 2004, p. 644) for handling information security. The connection is made between corporate governance and information security by internal controls (von Solms, 2000, p. 217). The boards' responsibility of due care is seen to apply to information as well (von Solms and von Solms, 2006b) and these responsibilities are discharged through the so called direct-control cycle (von Solms and von Solms, 2006a). Moulton and Coles note however that "*security governance is still a mess. It is poorly understood and ill defined, and therefore means different things to different people*" (Moulton and Coles, 2003, p. 580).

The above quote highlights the core problem of "information security governance". Although a significant amount of literature exists for information security at different levels, literature about governing information security is relatively thin, possibly as this field seems to be on the periphery of many different fields. This might be due partially to the view that information security is a technical issue (von Solms and von Solms, 2004), relating especially to computers.

In order to avoid the confusion apparent in the "information security governance" field this paper focused on corporate governance, especially on board activities. The main purpose of the investigation was to identify the Board responsibilities in regard to information security. The study was built around agency theory and the instruments reflected such a position. Furthermore, this study took the position that such a separation of governance and management should be made and deliberately included questions aimed at verifying whether such position can be supported. The research design accommodated such verification and is discussed in the following section.

RESEARCH DESIGN

In this study, a variant of the Delphi method (Dalkey & Helmer, 1963, Linstone & Turoff, 1975) was used for data collection. This method is applicable not only for forecasting (Czinkota & Ronkainen, 1997; Hayne & Pollard, 2000), but also for theory development (Bacon & Fitzgerald, 2001, Holsapple & Joshi, 2002; Mulligan, 2002).

The Delphi method was selected over other data collection methods because of its applicability to complex problems where reliable consensus of opinion is needed and incomplete knowledge exists about the phenomenon. Delphi is a proven method in these circumstances and has been practised by business and information technology researchers throughout the past four decades (Niederman et al., 1991, Peffers and Tuunanen, 2005, Keil et al, 2002, Brungs and Jamieson, 2005).

The aim of this research, however, was not necessarily to reach a consensus as is the general aim of the Delphi method, but simply to gather experts' opinions about the research area, thus enabling concept development. This approach is also a valid and recognised use of the Delphi method (Linstone and Turoff 1975, Bacon and Fitzgerald 2001, Holsapple and Joshi 2002, Okoli and Pawlowski 2004).

The original plan was to employ two Delphi panels: one of industry experts comprising 15-30 people, and another one of 6-8 corporate governance practitioners. The first cycle is completed; the second cycle is in progress. While the composite Delphi cycle will add significant value to the investigation, the initial results are worth considering and are discussed in this paper.

Industry experts were selected from a wide circle. Expertise was determined by publication, by conference activities, by position filled (past and present) and by general contribution to the particular field. As the research looked at overlapping areas of organisational and technology management, experts from each field were selected. The expert panel consisted of the following groups:

- Auditors
- Business leadership experts
- Business strategy consultants
- Corporate governance experts
- CPAs
- Information security experts
- IT management experts
- Partners of "the big 4" consultancy firms
- Risk consultants

By inviting two to three people from each group a panel was created where different views of governance were well represented. An important aspect of the panel size is the ability to balance and mitigate participants' personal characteristics such as outspokenness or timidness. It is important not only to balance the bias that comes from the represented profession, but also to avoid dominance of one person or a small group even if the discussion happens online. Since the suggested size of a Delphi panel is 7-30 people (Allen, 1978, Dalkey, 2003), a panel of 25 people was both manageable and representative.

As discussed above, the purpose of this study was not necessarily to reach a consensus, but to gather opinion. It can be argued that this is a legitimate method to accumulate data for the purpose of the Delphi method is "*to handle opinions rather than objective facts*" (Schmidt, 1997 cf Dalkey & Helmer, 1963). The opinions collected in the first Delphi cycle offer significant insights into the validity of the industry calls. The responses collected were compared and contrasted and an emergent picture was identified as described and discussed in the next section.

RESULTS AND DISCUSSION

Due to geographical distances – participants lived or worked in North America, Europe, Asia and Australia – the questions were administered via email. Since the issue investigated is of "global/international" scale, experts needed to be selected at international level. Originally 30 people were contacted, but five people couldn't fit participation into their schedule. The 25 participants were sent the first set of questions which consisted of a ranking exercise (ranking nine board level activities in order of importance) and four short questions.

- Question 1 probed the participants' understanding of corporate governance;
- Question 2 explored that further in the context of information security inquiring about the participants' views on information security and IT governance.
- Question 3 explored views on where governance and management separated while
- Question 4 queried the relationship between information security and corporate governance.

Although each question generated interesting responses, this paper focuses only on Question 4. Question 1-3 were needed to ascertain from the responses the context in which the analysis was going to be based on.

All 25 participants responded. This was an overwhelming response and more than adequate within the limit of the recommended size of a Delphi group. The responses were collated, analysed and fed back for further comment based on the composite result. This procedure was repeated to adequately clarify points of views.

The second round was conducted using an RASCI chart. Only eight of the original 25 responded, a sample close to the lower limit of the recommended Delphi group size, but still within the limit. However, the second round's purpose was only to verify the emergent picture of the first round. This purpose was achieved even with the smaller number of respondents (Allen, 1978, Schmidt, 1997).

The ranking exercise was connected to the fourth question, its purpose being to check the practical and theoretical view of participants. Either the ranking or the fourth question can be viewed and evaluated independently; together however they provide deeper insight into the phenomena.

Similarly questions 1 and 3 were linked together. Again, the composite result to the two questions provides a deeper insight than the individual responses.

Importance Ranking

The ranking exercise of the first round asked participants to rank nine activities – undertaken by corporate governance practitioners – in order of importance (See Table 1 – Importance ranking). Information security was included as part of the nine activities. Participants were also allowed to make suggestions for extra activities they considered important to be included in the ranking. The ranking followed the Mann-Whitney method (Mann & Whitney, 1947) to provide an accurate composite view and was checked for validity by a statistics expert from Columbia University. The group's consensus was that leadership and envisioning were the two most important aspects, while information security was ranked as being one of the lowest in importance.

Ranking on importance		
A set of characteristics of corporate governance activities are listed below in alphabetical order. Please rank them in order of priority of importance for corporate governance. Use the right hand side column for your list. If there are other characteristics that do not fit into any of the listed ones, please list them in the empty spaces provided.		
1	Capability and capacity creation	7
2	Disclosure	3
3	Environmental Scanning	9
4	Ethics	6
5	Information Security	10
6	Leadership / Envisioning	5
7	Performance measurement	8
8	Regulatory requirements	2
9	Risk minimisation/management	1
10	Strategy	4
11		
12		
Optional If you added other characteristics that do not fit into any of the listed ones, you may wish to provide a case for your selection. Please use the space provided below to make the case for your addition or for your order selection.		
Ensuring the efficacy of management's business strategy is fundamental to exercising the board's fiduciary responsibility.		

Table 1 - Importance ranking

Responses to Questions

Following the ranking, short questions probed the participant's understanding about corporate governance's relationship to information security. The first interesting result was that the majority of participants indicated that information security was considered essential for the board to fulfil their obligations. This was in sharp contrast to the ranking exercise. When explored further in the feedback, the emergent picture was that a difference exists between information security being essential to board practices and boards actually dealing with information security directly. This fits well within agency theory; therefore it can be argued that the role of information security in corporate governance and the board's role in information security are two distinct roles. The former can be seen to focus on ensuring the level of reliability and quality of information required at board level. The latter can be considered as setting the legal/ethical boundaries; the culture of information security within the organisation.

Another question probed the participants' view on the difference between governance and management. The majority of responses identified a difference indicating that management was an operational activity, while governance was direction setting and controlling. This was similar to the views expressed in literature (von Solms, 2000, Posthumus and von Solms, 2004) and confirmed our starting position.

Ambiguous Views on Governance

The relationship between governance and management, however, was somewhat ambiguous. An emergent picture indicated that corporate governance had lower and higher levels. The former was practiced by executive management – the CxOs of the corporation – while the latter was practiced by the board. The lower level of governance included such activities as strategy, policy setting and so on. The higher level practice included ethics, disclosure, setting legal and regulatory boundaries and the like. This separation is not clearly present in literature, possibly because current literature doesn't seem to make such a distinction. Investigating the concept further to clarity the issue should increase our understanding of corporate governance.

A small number of respondents suggested that governance was a subset of management. While exercised by the board, governance actually replicated the activities of management at a higher level of abstraction. Although there are pointers to such a view in organisational theory, it is most likely a very narrow interpretation of early corporate governance literature (Berle and Means, 1932). The view was vigorously contested by the majority of participants on both practical and theoretical grounds. This particular view doesn't fit into agency theory and

thus should be rejected. Governance is distinct from management (Tricker, 1994, Mueller, 1979), and should not be considered as the same at a higher, abstract level.

Gap in Views on Board Accountability

The relevance of information security and its relationship to corporate governance was further explored in the subsequent feedback. A consensus emerged that "*information security issues are of direct relevance to the corporation and its shareholders*." There was also an agreement that information security is "*superior, rather than subordinate, to 'technology' issues*". The differences mostly relate to the degree of importance and the way it could fit into governance and what should be done at board level.

Many industry experts – especially auditors, IT management experts and information security practitioners (group 1) – asserted that the board is responsible for information security practices. However, when asked for justification, the responses were vague. Information reliability as fundamental to the business required board attention was the most common answer, but this did not address the responsibility of the board. Further investigation is required to establish why group 1 characteristically held such a view without being able to explain why. The view however was challenged by corporate governance and business leadership experts (group 2). They suggested that information security management was an operational issue, thus not the accountability of the board. The small number of responses received from directors of boards vehemently supported the opinion of the corporate governance experts. The different views were not reconciled as both sides maintained their views. The emergent picture is that a gap exists between information security and IT practitioners and corporate governance practitioners. It can also be contended that the former group has departed from agency theory. One might conclude that such departure lacks a theoretical underpinning and is difficult to justify.

The implications of such departure are far reaching. It could be argued that most IT professionals do not have formal exposure to the underpinnings and practice of corporate governance. Further, an assertion could be made that there is very little awareness and understanding among most IT professionals regarding the functions, roles and activities of the board. This raises concerns regarding the consistencies and assumptions that underpin this view. Arguably, this lack of understanding has resulted in ill-defined governance (Hamaker 2003a and 2003b) and is the cause of confusion identified earlier in the IT audit profession. Further study about these phenomena is suggested about these phenomena in order to clear up misconceptions and misunderstanding, which are beyond the scope of this paper.

Delphi, Round Two – The RASCI Chart

The gap was further emphasised by the results of the second round. An RASCI chart was compiled listing 26 activities (Table 3 – RASCI chart 1 and Table 4 – RASCI chart 2)related to information security. For each activity participants were asked to select who was accountable, who was responsible; who had a supportive role; and who needed to be consulted or informed. The role and responsibility definitions are shown below (Table 2 – RASCI definitions):

Board	(identifies the chief governing body of people appointed to the office of corporate director)
Board Committee	(undertakes detailed reviews of items brought before the full Board for consideration and assist the Board to fulfil its duties. Can be supervisory or advisory.)
Executive Management	(high ranking corporate officers in charge of the total management of the whole company – such as CEO, COO, CFO, CTO, etc.)
Line Management	(administers the daily, operational activities contributing directly to the output of the company)

The responsibilities are the general RASCI types, with the adjusted terminology:

R	**Responsible**	(the "Doer", who actually does the Practice Area, or part of it. There can be multiple roles responsible)
A	**Accountable**	(is ultimately answerable for the decisions or for the completion of the Practice Area. **There must be exactly one A specified for each Practice Area**)
S	**Supportive**	(provides resources or demonstrates support for the Practice Area to be completed.)
C	**Consulted**	(is "in the loop" to provide information or capability necessary to complete the Practice Area in a 2 way communication.)
I	**Informed**	(is "kept in the picture" after a decision or action taken in a 1 way communication.)

Table 2 - RASCI definitions

Group 1 participants in general assigned accountability and responsibility to the board for most activities.

Practice Area	Board	Board Committee	Executive Management (CxO)	Line Management	Comments
Establish risk boundaries, such as risk appetite and risk tolerance	A, R	S, C	R, C	I, S	
Establish purpose, relevance, strategic direction of information security portfolio	A, R	S, C	R, C	I, S	
Establish information security principles for the organisation	A, R	S, C	R, C	I, S	
Set the information security culture	A, R	S, C, R	R, C	I, S, R	
Create decision making hierarchy	A, R	S, C, R	R, C	I, S, R	
Demonstrate support to information security initiatives	A, R	S, C, R	R, C	I, S, R	
Define constrains (legal, ethical, etc.) within which to operate	A, R	S, C	R, C	I, S	
Set expected return in information security investment	A, R	S, C	R, C	I, S	
Measure and compare expected and actual performance	S,	S, C	A, R, C	R, S	
Obtain assurance on adequacy of information security	A, R	S, C	R, C, S	R, C, S	
Acquire and mobilise resources	A, R	S, C	R, C, S	I	
Define scope and charter for security organisational elements	A, R	S, C	R, C, S	I, S	
Approve information security budget	A, R	S, C	R	I	
Create measurement criteria	S, C	S, C	A, R, C	R, S	
Create performance metrics of information security	S, C	S, C	A, R, C	R, S	
Set expectations from audit	A, R	S, C	R, C	I	
Evaluate return on information security investment	A, R	S, C	R, C	I	
Initiate discussions about information security on the Board	A, R	S, C	R, C, S	I, S	
Align information security strategy with business strategy	S, C	S, C	A, R, C	I	
Demonstrate sufficient information security to externals	A, R	S, C	R, C, S	R, S	
Establish information security organisation	A, R	S, C	R, C	I	
Create information security decision making rights	A, R	S, C	R, C	I	
Create information security budget	A, R	S, C	R, C	I	
Establish security awareness training	A, R	S, C	R, S, C	R, S	
Determine required capabilities and investment	A, R	S, C	R, S, C	I	
Become informed (of role and impact) about information security	A, R	R	R	R	
Ensure information security receives appropriate attention	A, R	R, S, C	R	R	

R = Responsible → → A = Accountable → → → S = Supportive → → → C = Consulted → → → I = Informed

Table 3 – RASCI chart 1

This assignment of accountability may be justified by saying that the board has the ultimate accountability for what the corporation does. Yet, this is considerably more difficult to justify in terms of responsibility. The board has neither the time, nor the resources, nor is and its focus so management-oriented. These aspects were reflected in the responses of Group 2 participants, which is shown below.

Practice Area	Board	Board Committee	Executive Management (CxO)	Line Management	Comments
Establish risk boundaries, such as risk appetite and risk tolerance	A	R	R C	I	The C-level might be consulted and /or responsible for aspects of this.
Establish purpose, relevance, strategic direction of information security portfolio	I	I	A R	R	This is a management function. The C level is accountable and may share responsibility with line management
Establish information security principles for the organisation	I	I	A R	R	This is a management function. The C level is accountable and may share responsibility with line management
Set the information security culture	I	I	A R	R	This is a management function. The C level is accountable and may share responsibility with line management
Create decision making hierarchy			A R	R	Assuming you mean decision making around incident handling, this is a management function. The C level is accountable and may share responsibility with line management. The board likely doesn't need to know the details.
Demonstrate support to information security initiatives		I S	A R	R	This is a management function. The C level is accountable and may share responsibility with line management. I'd think any board committee tasked with IT or security might be informed and/or demonstrate support.
Define constrains (legal, ethical, etc.) within which to operate	A	R	R	S	This is a hard one to score. The board will certainly be concerned about ethical issues and other entity level issues such as regulatory compliance. I'd hold them accountable with any board committees, and C-level responsible with line management supporting.
Set expected return in information security investment			A R	R	This should be management
Measure and compare expected and actual performance	I	I	A R	R	This is management but the Board *may* be interested in performance but maybe not at this level. I think it, for the Board may depend on the Board.
Obtain assurance on adequacy of information security		I	A R		I think this is a management task. A board level committee might be tasked with tracking such as the Audit Committee. That might make them A R in that case.
Acquire and mobilise resources			A R	R	This should be management *unless* it means getting an independent auditor.
Define scope and charter for security organisational elements			A R	S	Mainly executive management with support from line management
Approve information security budget			A R	S	Mainly executive management with support from line management
Create measurement criteria		C I	A R	S	Mainly executive management with support from line management. A committee such as the Audit Committee may have particular metrics they want to see. Again, I think this would depend on the Board.
Create performance metrics of information security		C I	A R	S	Mainly executive management with support from line management. A committee such as the Audit Committee may have particular metrics they want to see. Again, I think this would depend on the Board.
Set expectations from audit		C	A R	S	Management should work with the audit committee, internal and external audit to understand *and* set expectations.
Evaluate return on information security investment	I	I	A R	S	This is management but the Board *may* be interested in performance but maybe not at this level. I think it, for the Board may depend on the Board.
Initiate discussions about information security on the Board	A	R	R	S	This is hard if you only want one "A" here. The Board should create an environment wherein they can request information security to present *or* if something is important enough. Management should be able to request an audience. I decided to put the "A" on the Board as it is up to them to create a culture wherein they are approachable.
Align information security strategy with business strategy	I	I	A R	S	This is management but the Board *may* be interested in performance but maybe not at this level. I think it, for the Board may depend on the Board.
Demonstrate sufficient information security to externals	I	I	A R	S	To external what? External Auditors? Investors? Regardless, this is a management task though the Board may want to know it is going on.
Establish information security organisation	I	C I	A R	S	A & R resides with senior management. They may consult or inform the audit committee or another appropriate committee.
Create information security decision making rights			A R	S	Management
Create information security budget			A R	S	Management
Establish security awareness training			A R	S	Management
Determine required capabilities and investment			A R	S	Management
Become informed (of role and impact) about information security	A/R	R	R	S I	The Board and Management must understand their role and tell lower levels what their role is or work with them to define it. I felt this was a "tone from the top" issue and thus set accountability with the Board to ensure their role is understood and then work with senior management. It would then waterfall downwards.
Ensure information security receives appropriate attention	A/R	R	R	S	Again, this would seem to be important to set from the top. Some boards may see this as a management issue and tell them to get it done. Other Boards may take a few high-level steps to make sure that management continues to pay proper attention. Ultimately, day to day management of information security *is* a management responsibility. The Board may just want to be informed. The structure would depend on the board.

Table 4 - RASCI chart 2

The two views were impossible to reconcile. This is another strong indication that a significant gap exists in regards to boards of directors' role and responsibility between IT and information security experts and corporate governance experts. As pointed out earlier, this gap is most likely due to a departure from agency theory and/or incorrect understanding (Hamaker, 2003a, 2003b) of corporate governance.

The View Taken

Since there are many inconsistencies and misconceptions in the views held by information security and IT experts, this paper considers the view of corporate governance experts as the more appropriate one. The gap however can be narrowed from both sides. Corporate governance experts need to consider changing boundaries and emerging issues such as privacy and reliability (which are major concepts in information security). Information security experts need to familiarise themselves with the theoretical and legal underpinnings of corporate governance. Since corporate governance's boundaries and responsibilities defined by law, an approach that takes legal requirements and theoretical underpinnings into consideration is the best approach.

As discussed earlier, the study has not been completed yet. The early indication is that information security and IT experts have a differing view on corporate governance from the corporate governance practitioners themselves. This differing view can cause a number of anomalies. It can be contended that each anomaly needs to be investigated and evaluated on its own merit. However, existing theories need to be considered and new views integrated with those existing theories. It can also be contended that in case of differing and irreconcilable views the one that has stronger theoretical underpinnings should prevail.

CONCLUSION

The validity of the claim that information security governance is the responsibility of the board needs further investigation. The aspects of due care, due diligence and vicarious liability need to be considered and compared to the three underlying concepts (individual's rights, market and ethical behaviour) of corporate governance. It is most likely that information security has a role in corporate governance but that role has to be clearly identified and integrated within a corporate governance framework.

The results of the described study highlight the importance of considering the underlying theory of corporate governance when discussing the topic of governance in general and in relation to boards of directors' responsibilities. The emergent picture is that operational-type activities are expected from the boards of directors by certain industry groups; therefore the separation between senior management and the board is blurred. The term "governance" seems to be used differently for IT governance and information security governance by those industry bodies. The etymological roots are abandoned, and the usage is not always consistent with the usage in corporate governance literature.

Since corporate governance is enshrined in law (Baxt, 1982, Berle and Means, 1932), care must be taken and changes can't be suggested or made arbitrarily. It can be argued that anything advocated as the boards of directors' responsibility must fit into the theoretical frameworks and underpinnings of corporate governance. Similarly, governance and management need to be clearly separated in order to understand the context of information security and IT governance. The provisional findings of this study suggest that information security governance or IT governance should be approached from a corporate governance framework rather than the other way around.

REFERENCES

Albanese, R., Dacin, M. T., Harris, I. C., Davis, J. H., Schoorman, F. D., Donaldson, L. (1997) Dialogue, *Academy of Management Review*, 22(3), 609-613.

Allen, T. H. (1978) *New methods in social science research: Policy sciences and future research*, Praeger Publishing, New York.

ASX, 2003, Principles of Good Corporate Governance and Best Practice Recommendations, URLhttp://asx.ice4.interactiveinvestor.com.au/ASX0301/Principles%20of%20Good%20Corporate%20Governance/EN/body.aspx?z=1&p=1&v=1&uid=, Accessed 4 Aug 2008.

Bacon, D., Fitzgerald, B. (2001) A systemic framework for the field of information systems, *Database for Advances in Information Systems* 32(2), 46–67.

Baxt, R. (1982) *Duties and Responsibilities of Directors and Officers*, Australian Institute of Corporate Directors (AICD), Sydney, Australia, 17th Edition, 2002, 45-82.

Berle, A. A. and Means, G.C. ([1932] 1968) *The Modern Corporation and Private Property*, New York: Harcourt, Brace & World.

Bernstein, W. J. (2004) *The birth of plenty: how the prosperity of the modern world was created*, McGraw-Hill Companies Inc., New York.

Bhagat, S., and Jefferis Jr., R.H. (2005) *The Econometrics of Corporate Governance Studies*, MIT Press, USA, p.14.

Boyd, B. (1990) Corporate Linkages and Organizational Environment: A Test of the Resource Dependence Model. *Strategic Management Journal* 11(6), 419-430.

Brungs, A. & Jamieson, R. (2005) Identification of legal issues for computer forensics, *Information Systems Management*, 22(2), 57 - 66.

Byrson, J.M. (2004) What to do when stakeholders matter, *Public Management Review*, 6(1), 21-53.

Bryson, J. M., Cunningham, G. & Lokkesmoe, K. L. (2002) What to Do When stakeholders Matter: The Case of Problem Formulation for the African American Men Project of Hennepin County, Minnesota. *Public Administration Review*, 62(5), 568-584

BSA (Business Software Alliance), (2003) *Information Security Governance: Toward a Framework for Action*, Business Software Alliance, URL www.globaltechsummit.net/press/ISGPaper-2003.pdf, Accessed 17 May 2004.

Cadbury, A. (1992) *The Financial Aspects of Corporate Governance*, Gee and Co. Ltd., London, UK. p. 14

Chew & Gillan (2005) *Corporate Governance At The Crossroads*, McGraw, Hill, Irwin.

CGTF (Corporate Governance Task Force) Report, (2004) *Information Security Governance, A Call to Action*, National Cyber Security Summit Task Force, URL www.cyberpartnership.org/InfoSecGov4_04.pdf , Accessed 17 May 2004.

CICA (Canadian Institute of Chartered Accountants), (2004) *20 Questions Directors Should Ask About IT*, Toronto, Canada.

CIMA, (2004) *Enterprise Governance - Getting the Balance Right*, International Federation of Accountants, URL www.cimaglobal.com/downloads/enterprise_governance.pdf, Accessed 16 May 2004,

Czinkota, M.R. and Ronkainen, I.A. (1997) International business and trade in the next decade: report from a Delphi study, *Journal of International Business Studies*, 28(4), 827–844.

Coase, R. (1937) The nature of the firm, *Economica*, 4(16), 386-405

Cochran, P.L. and Wartick, S.L. (1988) *Corporate Governance: A Review of the Literature*, Financial Executives Research Foundation, New Jersey, USA.

Colley, Jr., J.L.; Doyle, J.L.; Logan, G.W. & Stettinius, W. (2003) *Corporate Governance*, McGraw-Hill, New York.

Corporate Law Economic Reform Program also known as Audit Reform and Corporate Disclosure Act 2004 (CLERP), URL http://scaleplus.law.gov.au/html/pasteact/3/3673/pdf/1032004.pdf Accessed 4 Aug 2008.

Dalkey, N, and Helmer, O. (1963) An Experimental Application Of The Delphi Method To The Use Of Experts, *Management Science*, 9(3), 458-467

Dalkey, N. C. (2003) *The Delphi Methodology*, URL http://www.fernunihagen.de/ZIFF/v2-ch45a.htm, Accessed 10 Nov 2005.

Davis, J. H., Schoorman, F. D., & Donaldson, L. (1977) Toward a stewardship theory of management, *Academy of Management Review*, 22(1), 20-47.

Declaration of Independence (1776) URL http://www.ushistory.org/declaration/document/index.htm, Accessed 4 Aug 2008.

Dey (1994) *Where Were The Directors? Guidelines for Improved Corporate Governance in Canada (The Toronto Report)*, The Toronto Stock Exchange, URL http://www.ecgi.org/codes/documents/dey.pdf Accessed 4 Aug 2008.

Donaldson, L. (1990) The ethereal hand: Organizational economics and management theory, *Academy of Management Review*, 15(3), 369-381.

Donaldson, L., Davis J.H. (1991) Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns, *Australian Journal of Management*, 16(1), 49-66.

Donaldson, T. and Preston, L.E. (1995) The Stakeholder Theory of the Corporation: Concepts, Evidence and Implications, *Academy of Management Review*, 20(1), 65-91.

Eisenhardt, K. M. (1989) Agency theory: An assessment and review. *Academy of Management Review*, 14(1), 57-74

Fama, E. F. and Jensen, M. C. (1983) Separation of Ownership and Control, *Journal of Law and Economics*, 26 301-325.

Firstenberg, P. B; Malkiel, B. G. (1994) The Twenty-First Century Boardroom: Who Will Be in Charge? *Sloan Management Review*, 36(1), 27-35.

Freeman, R. E. (1984) *Strategic management: A stakeholder approach*, Pitman, Boston, MA, USA.

Geer, D. E. (2004) Why Information Security Matters, *Cutter Consortium Business-IT Strategies* 7(3).

Hamaker, S. (2003a) Spotlight on Governance, *Information Systems Control Journal*, 1, ISACA, Rolling Meadows

Hamaker, S. (2003b) Principles of Governance, *Information Systems Control Journal*, 3, ISACA, Rolling Meadows

Hayne, S., and Pollard, C. (2000) A comparative analysis of critical issues facing Canadian information systems personnel: a national and global perspective, *Information & Management* 38(2), 73–86.

Hayward, M. L. A. and Boeker, W. (1998) Power and Conflicts of Interest in Professional Firms: Evidence from Investment Banking. *Administrative Science Quarterly*, 43(1), 1-22.

Holsapple, P. and Joshi, K. (2002) Knowledge manipulation activities: results of a Delphi study, *Information & Management*, 39(6), 477–490.

Institute of Internal Auditors (IIA), (2001a) *Information Security Governance: What Directors Need to Know*, Institute of Internal Auditors, and The Critical Infrastructure Assurance Office, US Dept. of Commerce, URL http://www.theiia.org/?doc_id=3061, Accessed 17 May 2005.

ITGI 1(IT Governance Institute), (2001) *Information Security Governance: Guidance for Board of Directors and Executive Management*, IT Governance Institute (ITGI), URL www.itgi.org, Accessed 17 May 2005.

ITGI 2 (IT Governance Institute), 2003, *IT Governance Executive Summary*, URL www.itgi.org, Accessed 18 April 2004.

Jensen, M. C, & Meckling, W. H. (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360.

Jensen M. C., and Ruback, R. S. (1983) The Market for Corporate Control: The Scientific Evidence, *Journal of Financial Economics*, 11(1), 5-50.

Keil, M., Tiwana, A. & Bush, A. (2002) Reconciling user and project manager perceptions of IT project risk: A Delphi study. *Information Systems Journa*l, 12(2), 103 - 119.

Larner, R. J. (1970) *Management Control and the Large Corporation*, Dunellen, New York.

Linstone, H. A. and Turoff, M. (1975) *The Delphi Method: Techniques and Applications*, Addison-Wesley, London.

Lorsch, J. W. and McIver, E. A. (1989) *Pawns or Potentates: The Reality of America's Corporate Boards*, Harvard Business School Press, Boston.

Mann, H. B., and Whitney, D. R. (1947) On a test of whether one of two random variables is stochastically larger than the other, *Annals of Mathematical Statistics*, 18, 50-60.

Millstein, I.M. (2004) *The Accountable Corporation A Perspective On Corporate Governance (Rules, Principles, or Both)*, URL http://millstein.som.yale.edu/speech_search/, Accessed 26 July 2008.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997) Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *Academy of Management Review*, 22(4), 853-886.

Monks, R.A.G. and Minow, N. (2001) *Corporate Governance*, 2d Edition, Blackwell Publishing.

Monsen, J. R., Chiu, J. S. and Cooley, D. E. (1968) The Effect of Separation of Ownership and Control on the Performance of the Large Firm, *Quarterly Journal of Economics* 82(3) 435-451.

Moulton, R. and Coles R. S. (2003) Applying information security governance, *Computers & Security*, Amsterdam, 22(7), 580-584.

Mueller, R. K. (1978) *New directions for directors*, DC Heath & Co, Lexington, Massachusetts.

Mueller, R. K. (1981) Changes in the wind of corporate governance, *Journal of business strategy*, 1(4), 8-14.

Mulligan, P. (2002) Specification of a capability-based IT classification framework, *Information & Management* 39(8), 647–658.

NASB (1995) *New American Standard Bible*, The Lockman Foundation

Niederman, F., Brancheau, J. C., & Wetherbe, J. C. (1991) Information systems management issues for the 1990s. *MIS Quarterly*, 15(4), 475 - 500.

Okoli, C. and Pawlowski, S. D. (2004) The Delphi method as a research tool: an example, design considerations and applications, *Information & Management*, 42(1), 15–29

Peffers, K. & Tuunanen, T. (2005) Planning for IS applications: A practical, information theoretical method and case study in mobile financial services, *Information & Management*, 42(3), 483-492.

Pfeffer, J. (1982) *Organizations and Organization Theory*, Pitman, Boston, USA.

Posthumus, S. and von Solms, R. (2004) A framework for the governance of information security, *Computers & Security*, Amsterdam, 23(8), 638-646.

Rowley, T. J. (1997) Moving Beyond Dyadic Ties: A Network Theory of Stakeholder Influences. *Academy of Management Review*, 22(4), 887-910.

SAI, 2003, AS 8000-2003 Corporate governance - Good governance principles, URL http://www.saiglobal.com

Sarbanes-Oxley Act of 2002, URL http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf ,Accessed 4 Aug 2008.

Sackman, H. (1975) *Delphi Critique: Expert Opinions, Forecasting, and Group Process*, D. C. Heath, Lexington, MA, USA.

Shleifer, A. and Vishny, R (1997) A Survey of Corporate Governance, *Journal of Finance*, 52(2), 737-783.

Schmidt, R. C. (1997) Managing Delphi surveys using nonparametric statistical techniques, *Decision Sciences*, 28(3), 763-774.

Smith, A., 1759, The Theory of Moral Sentiments, URL http://www.ibiblio.org/ml/libri/s/SmithA_MoralSentiments_p.pdf, Accessed 4 Aug 2008.

Smith, A. (1776) An Inquiry into the Nature and Causes of the Wealth of Nations, Vol. II. ed. A.S. Skinner and R.H. Campbell, *vol. III of The Glasgow Edition of the Works and Correspondence of Adam Smith, Indianapolis*: Liberty Fund, 1981.

Taylor, F.W. (2002), *Critical evaluations in business and management*, Routledge, London, p.59.

Tricker, R.I. (1984) *Corporate Governance*, Gower, London.

Tricker, R.I. (1994) *International Corporate Governance: Text Readings and Cases*, New York, Prentice Hall, p.149.

von Solms, B. (2000) Information security - The third wave? *Computers & Security*, Amsterdam, 19(7), 615-620.

von Solms, B. and von Solms, R. (2004) The 10 deadly sins of information security management, *Computers & Security*, Amsterdam, 23(5), 371-376.

von Solms, B. and von Solms, R. (2006a) Information Security Governance: A model based on the Direct–Control Cycle, *Computers & Security*, Amsterdam, 25(6), 408-412.

von Solms, B. and von Solms, R. (2006b) Information security governance: Due care, *Computers & Security*, Amsterdam, 25(7), 494-497.

Weber, M. (1930) *The Protestant Ethic and the Spirit of Capitalism*, Routledge, London, UK.

Weiss, A.R. (1995) Cracks in the Foundation of Stakeholder Theory, *Electronic Journal of Radical Organisation Theory*, 1(1).

Westby, J. (2004) *Information Security: Responsibilities Of Boards Of Directors And Senior Management*, Testimony Before the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, 22 Sept 2004, URL http://reform.house.gov/UploadedFiles/Westby1.pdf, Accessed 22 Nov 2004.

Williamson, O.E. (1979) Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics*, 22(2), 233-261.

Williamson, O.E. (1981) The economics of organization: The transaction cost approach. *The American journal of sociology*, 87(3), 548-577.

Zeitlin, M. (1974) Corporate Ownership and Control: The Large Corporation and the Capitalist Class, *American Journal of Sociology* 79(4), 1073-1119.

COPYRIGHT