Spring 6-20-2012

Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations

Janine Holgate
Wipro Technologies, janine.holgate@wipro.com

Susan P. Williams
University of Koblenz-Landau, Germany, susan.williams@uni-koblenz.de

Catherine A. Hardy
The University of Sydney, Australia, catherine.hardy@sydney.edu.au

25th Bled eConference

eDependability:

Reliable and Trustworthy eStructures, eProcesses, eOperations

and eServices for the Future

June 17, 2012 – June 20, 2012; Bled, Slovenia

Information Security Governance: *Investigating Diversity in Critical Infrastructure Organizations*

Janine Holgate

Wipro Technologies

janine.holgate@wipro.com

Susan P Williams

University of Koblenz-Landau, Germany

susan.williams@uni-koblenz.de

Catherine A Hardy

The University of Sydney, Australia

catherine.hardy@sydney.edu.au

Abstract

The aim of this paper is to report on how information security governance (ISG) arrangements are framed and shaped in practice. Our objective is to examine the extent to which the similarities and differences in institutional environments can subject organizations to multiple, competing and even contradictory arrangements for ISG. Using an interpretive case based research strategy we investigate how ISG arrangements are framed and shaped in fourteen critical infrastructure organizations in Australia. We explicitly recognize the socio-technical nature of ISG and draw insights from institutional theory. Our findings illustrate the heterogeneity and malleability of ISG across different organizations and highlight the need for an information centric view.

Keywords: information security governance, critical infrastructure, interpretive case study

1 Introduction

Information security governance (ISG) is increasingly recognized as a critical issue for organizations in terms of accountability, fiduciary duties and delivering value [ITGI 2011]. Theft, destruction or unauthorized access to an organization's information technology (IT) and information assets arising from malicious actions, inadvertent errors or natural or man-made disasters, may result in compromised information, serious system disruptions, business continuity concerns, compliance breaches, reputational damage, and a loss of intellectual property, strategic opportunities and shareholder value. Hence there has been growing recognition in the scholarly literature [Baskerville & Siponen 2002; Dhillon 2007; Straub, Goodman & Baskerville 2008] and the practitioner literature [DTT 2007; ITGI 2008] over the past decade that technical solutions are necessary but not sufficient in meeting information security challenges. This has refocused attention from viewing information security as an operational responsibility concerned with technical infrastructure to an enterprise-wide and strategic business-led responsibility placing greater emphasis on business requirements, engaging the right people, employing the right technology and protecting critical information assets [E&Y 2009; Allen & Westby 2007].

A number of normative standards, prescriptive frameworks and models have been developed to assist in governing information security however no single framework is recognized or used universally [ITGI 2011:30]. Whilst the challenges of ISG are universal in terms of protecting information assets, the way each organization responds may vary according to its specific context, requirements and risk tolerance levels.

To date there has been limited empirical research directed at how the objectives of these standards and frameworks are actually achieved in organizations [Siponen 2006] and coordinated with other governance efforts. Further, greater understanding about how ISG is integrated in the organization and its internal and external influences is required. This has been identified as especially important in planning ISG audits [Love et al 2010].

In this paper we address these limitations and requirements and focus attention on the variations in arrangements for ISG. We present the findings and implications of a multi-case study of ISG arrangements in Australian critical infrastructure organizations. Our choice of critical infrastructure organizations as a context for studying ISG arrangements is based on two key factors. First, critical infrastructure protection is of national significance for the Australian Government [AGD 2010] providing a rich empirical context. Second, at a theoretical level it provides an opportunity to examine multiple organizations in an organizational field based on an issue rather than a product or market and to investigate the institutional logics that shape ISG in practice. The research is especially relevant to the Bled conference theme as ISG is part of an organization's efforts to ensure dependability and reliability in business operations.

The paper is organized as follows: in the next section we discuss recent developments in the area of ISG and draw out a socio-technical and institutional view of ISG. We then present the research aims and objectives, research approach and the key research findings. We conclude with a discussion of the implications of the findings for ISG and for enterprise information management more widely.

2 Changing perspectives on information security

A review of the literature reveals two discernible but overlapping streams of research in the study of information security. The first (and earlier) stream is largely technical in perspective and is concerned with the technologies and processes for securing information and IT assets. A limitation of this work was a lack of focus on understanding the social, organizational and human aspects of information security in relation to these technical aspects [Straub, Goodman & Baskerville 2008; Siponen & Willison 2007]. This led to calls for a "socio-organizational" or "socio technical" perspective [Dhillon & Backhouse 2001], echoing practitioner concerns for the need to shift attention "from an information-technology-based, security-centric, technology-solution perspective to an enterprise-based, risk management, organizational continuity and resilience perspective" [Allen 2005:29].

The second stream of research addresses this limitation and focuses attention on the need for a process oriented, strategic and organizational wide view [Straub, Goodman & Baskerville 2008:11, Allen 2005:11]. Hence more socially oriented studies such as organizational values in information security objectives [Dhillon & Torkzadeh 2006], outsourcing [Karyda, Mitrou & Quirchmayr 2006], institutional influences of information security [Hu, Hart & Cook 2007], developing information security strategy [McFadzean, Ezingeard & Birchall 2007] and formulating policy [Baskerville & Siponen 2002] have been conducted. The subject matter investigated in these studies reveals the problematic nature of ISG, where our discussion now turns.

2.1 Meaning and scope of ISG

Various definitions and understandings of the term "information security governance" (ISG) exist in the literature. For example, the IT Governance Institute [ITGI 2006:17] defines ISG as a "… subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security programme."

Allen [2005:6] viewed "governing for enterprise security" (GES) as building on and expanding "commonly defined forms of governance" which included enterprise, corporate and IT governance.

Other researchers recognize information security as a part of corporate and IT governance [McFadzean, Ezingeard & Birchall 2007; Von Solms 2005] or include aspects of governance in their discussions and categorize their work within the realm of information security management [Caralli 2004; Dutta & McCrohan 2002]. Thomson and von Solms [2005] view information security as having an overlapping function with corporate governance and corporate culture, adopting the term "information security obedience" to reflect the relationship between all three fields.

Thus, common understandings of ISG appear to be general in scope and to combine information security with existing conceptions of corporate and IT governance.

Such views provide limited insight into the relationship between information security and governance, assume there are similar goals and lack clarity as to the governance roles and responsibilities of senior management and board members with respect to

security concerns. Thus, the ISG literature recognizes information security as a governance issue. However, it is largely prescriptive, and provides limited empirical guidance; there remains a need to develop theory in ISG that looks beyond the newest "best practice" and provides contextually based understanding.

2.2 From a technical view to a socio-technical and institutional perspective

As identified above, the combining of information security with the concept of governance has resulted in the grouping of many heterogeneous elements without exploration of the interactions between these elements, raising two key issues.

First there is a recognized need identified by scholars in the information security literature to widen the analytic focus from a technically centric emphasis to incorporate a "socio-organizational" perspective [Straub, Goodman & Baskerville 2008; Hu, Hart & Cook 2007]. While this perspective has drawn attention to the importance of social contexts broadly, it remains unclear as to what the term 'socio' in socio-organizational stands for given the diverse disciplinary spaces that examine social dynamics. For example Dhillon and Backhouse [2001:147] view it broadly as investigations grounded in the interpretive paradigm to assist understanding of the organization and social world. They also appear to use the term interchangeably with "socio-technical" [ibid:p.140]. Hu, Hart and Cooke [2007] adopted a sociological neo-institutional approach to highlight the influence of institutional factors on organizational actions and behaviours, using a positivist case study approach.The socio-organizational view conveyed in the literature does not give sufficient consideration to what Orlikowski and Barley [2001:152] describe as the "material constraints and affordances of technologies" and ignores how social and technical elements are linked. We argue that a socio-technical systems (STS) perspective may assist in bringing further clarity to the field. We view STS as a set of theoretical principles providing insights into the reciprocally constitutive nature of social and technical systems [ibid:148]. That is "human and organizational outcomes [can] only be understood when social, psychological, environmental and technological systems are assessed as a whole" [Griffith & Dougherty 2001:205]. Further, certain features or types of technologies may necessitate different social arrangements [Pinch 2008: 468]. Hence, we ground the research approach of this study in social constructionism ideals.

Second, the extant literature is largely silent on how organizations actually engage with ISG related activities as the field is heavily populated with descriptive and prescriptive frameworks. From a socio-technical perspective, these normative models may be viewed as codified specifications that signal the arrangements and purpose of social and technical components and their relationship in information security. However, the role that such frameworks play in governing the protection of IT and information assets in organizations and how they manifest themselves in the way that organizations frame their governance arrangements remains under-explored, requiring greater empirical scrutiny and more contextually attuned theorizing.

We complement the STS view with an institutional perspective, to provide further insights into how technologies are embedded in complex social, economic and political settings and consequently shaped by such institutional influences [Orlikowski & Barley

2001]. In particular we explore the concept of institutional logic defined as "the socially constructed, historical patterns of material practices, assumptions, values, beliefs, and rules by which individuals produce and reproduce their material subsistence, organize time and space, and provide meaning to their social reality" [Thornton & Ocasio 2008:101]. For example information security, corporate governance and critical infrastructure may be viewed as three competing institutional orders which have different beliefs and practices that shape how individuals may engage in ISG.

3 Research approach

The study adopts an interpretive case study approach and is organized as follows.

3.1 Aims and objectives

Against the background of change in ISG outlined above and the adoption of a socio-technical systems stance we articulate our core research question as:

How are ISG arrangements framed and shaped in Australian Critical Infrastructure Organizations?

Our aim is to examine the extent to which the similarities and differences in these institutional environments can subject organizations to multiple, competing and even contradictory arrangements for ISG. We explicitly recognize the socio-technical nature of ISG and in doing so we move away from the question of what ISG is, to questioning how ISG arrangements are shaped and institutionalized in organizations that are themselves embedded in complex, changing socio-technical contexts. In support of this core research question we organized our investigation around three distinct, but inter-related sub-questions that assist us to understand and interpret contextual variations in ISG.

RQ1:What are the drivers and scope of ISG?

The objective of this question is to identify the range and variations in the key drivers and the scope or focus of ISG initiatives.

RQ2: Who are the owners of ISG?

The objective of this question is to establish the primary owner/responsible agency for ISG initiatives.

RQ3: Where is the locus of ISG?

The objective of this question is to establish the locus of ISG in relation to IT governance and corporate governance and its variation across different contexts.

In the following section we provide an overview of the research design and data collection methods.

3.2 Case study sites

All the companies included in the sample are critical infrastructure organizations. Critical infrastructure comprises the physical and cyber-based systems necessary for the efficient operation of economies and governments. In Australia, the following sectors are deemed to be critical infrastructure – energy, utilities, transport, communications,

health, food supply, finance, government services, national icons, and manufacturing. To draw out contextual variations we selected organizations from a range of these industries and from both the public and private sectors. The resultant sample comprises 6 private companies and 8 public companies. Specific information describing the case study sites and the key informants is provided in Table 1. Company names have been changed to maintain anonymity and to meet our research ethics protocol.

Company	Description	No. of Employees	Revenue	Key informants
Advantage	Integrate IT and telecommunications carrier, Australian and Asia Pacific	380	$228m	CEO/Director, GM Data & Security, Security Practice Mgr (+interim Info Security Officer)
Bank	Bank – Australia		$346.4m	Chief GM IT (CIO equivalent)
Best Practice Co	Retail water utility. State owned	357	$356.8m	GM Finance/Company Secretary, CIO
Consultant	Global provider of professional services	3724 (Aus)	$676m (Aus)	CIO Oceania
Differentiator	Information management company	600 (Aus)	$196.6m	CFO
Distributor	Electricity transmission provider. State owned.	974	$452.6m	CIO
Energy	Electricity generator. State owned.	363	$579m	MD/Director, IT/Communications Mgr, Risk Mgr.
Electrical	Retail/distribution electricity company. State owned.	984	$663m	CEO/Director, CIO, Non-exec director
Electricity	Retail/distribution electricity company. State owned.	2176	$1.3b	GM Regulatory & Corporate Affairs (including IT responsibility)
Healthy	Health insurer	1100	$1.9b	Group Executive (BU) (former CFO and acting CEO)
Retail Gas	Retail market administrator, virtual company.	2	n/a	CEO
Start-up	Newly formed, emergent gas production company	80+ contractors	$6m	COO, Executive Chairman
Water	Electricity generator, State owned.	870	$439.8m	CEO/Director, GM Corporate (including IT responsibility)
Virtual	Retail market administrator, virtual company.	1	n/a	CEO

Abbreviations:

CEO: Chief Executive Officer COO: Chief Operating Officer GM: General Manager
CIO: Chief Information Officer CFO: Chief Financial Officer MD: Managing Director
Mgr: Manager

Table 1: Case sites and key informant summary

3.3 Data collection and data reduction

Primary data were collected from 23 semi-structured interviews with Chief Executive Officers, Chief Information Officers and other senior officers, including executive and non-executive company directors at the 14 case study sites. All interviews were digitally recorded as audio files and subsequently transcribed into text files. In addition, secondary data comprising documents provided by the participants and publicly available information, contributed to the data collected. The primary aims of the research data analysis were to understand the cases themselves through the coding of the primary and secondary data to identify key themes and understand the relationships between them. Following Miles and Huberman [1994], a mixed data analysis approach comprising content analysis, thematic analysis and comparative analysis was adopted. This involved analyzing the data using codes and memos, reducing information via themes, and relating code categories. Within-case comparisons using coding techniques served as the basis for developing 14 individual organizational case studies, and cross-case comparison allowed for the identification of similarities and differences between the sample companies.

4 Findings

In the following sections we present our study findings. We organize their presentation around the three research sub-questions: drivers and scope of ISG, ISG ownership and locus of ISG**.**

4.1 Drivers and scope of ISG

Three distinct drivers of ISG were identified: 1. Legislation/Cyber Threat, 2. Business Continuity and 3. Strategic Differentiation (Figure 1). For all cases the most significant driver shaping ISG initiatives is regulatory compliance and protection against cyber threats.

As designated critical infrastructure organizations all the cases are subject to coercive regulatory pressures imposed by the Australian Federal and State governments. All cases have also been subject to normative pressures from institutional agents such as professional bodies, and/or by the existence of perceived “best practice” organizations. The only information security standard which has been fully adopted is ISO 17799 (now known as ISO 27002) by Advantage, and its Australian version AS/NZS 17799 (now known as AS/NZS 27002) by three other cases. The remaining cases have been guided by AS/NZS 7799 and have adopted various portions of this standard on a more informal basis, electing not to gain security certification. They also follow certain aspects of the COBIT and ITIL frameworks. ISG is generally driven through an amalgamation of other integrated processes such as risk management. Hence, other standards, such as AS 4360 (Risk Management, now known as AS/NZS ISO 31000) and ISO 9001 (Quality Management) and regulations and guidelines, such as the Australian Stock Exchange (ASX) Corporate Governance Council’s Principles of Good Corporate Governance and Best Practice Recommendations have been followed.

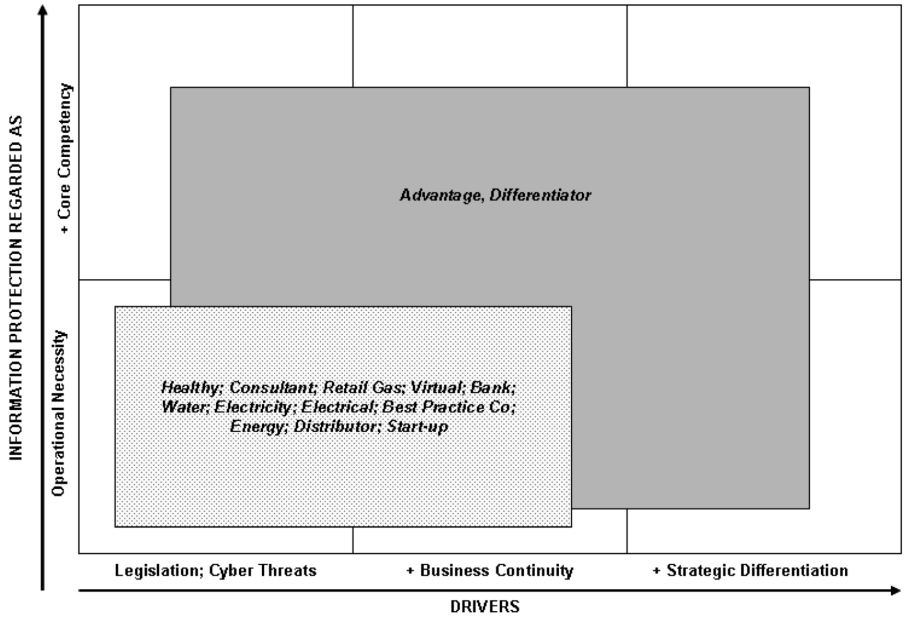

Figure 1: Drivers and scope of ISG

Whilst there is evidence of other drivers such as business continuity needs, customer imperatives and strategic differentiation, only two of the fourteen cases, Advantage and Differentiator have been influenced by all of these drivers. In both these cases information security is a core competency, as well as an operational necessity demonstrating a wider scope than the other cases, where the ISG focus is solely as an operational efficiency. Both Advantage and Differentiator have evolved and matured furthest toward an enhanced ISG capability, which includes a strategic and enterprise wide approach.

4.2 ISG Ownership

Two areas of ISG owenership were identified: IT executive and Business executive. The IT function executive retained primary responsibility in nine of the fourteen cases as shown in Table 2. In some instances at the Board level, there was a feeling that the Board members were not IT literate enough to own ISG. In these cases ISG was consequently delegated to the CEO; the CEO often then delegated the ownership of ISG to the executive responsible for IT. For the remaining five cases, the Business Executive for varying reasons owned ISG. For example, Start-up outsources its IT function, Virtual and Retail Gas are two virtual companies, and Advantage and Differentiator regard *'information protection'* as a core competency.

The use of the term information protection in the context of Advantage and Differentiator denotes they place a more significant emphasis on the information itself. The findings also highlight a different view from the widespread calls in the literature for more direct Board responsibility. They indicate that even though the respective Boards do maintain high-level oversight, Board level ISG leadership, management and control have been delegated to the Executive in all instances.

Case site	Primary owner: IT function Executive e.g. CIO	Primary Owner: Business Executive e.g. CEO
Energy	✓	
Electrical	✓	
Water	✓	
Electricity	✓	
Distributor	✓	
Healthy	✓	
Start-up		✓
Bank	✓	
Retail Gas		✓
Consultant	✓	
Differentiator		✓
Best Practice Co	✓	
Advantage		✓
Virtual		✓

Table 2: Summary of Primary Owners

The findings also revealed the holistic nature of ISG, in all cases, all individuals within an organization were expected to assume some level of responsibility for ISG; interestingly this is an issue that is given limited attention in the academic literature. Futher, whilst the Executive (including IT) and Board were the key actors defining the organizing principles and normative roles of this function, lower levels within the organization, as well as extra-organizational actors such as strategic partners and outsourcing companies have been drawn into the tactical arenas of ISG.

4.3 Locus of ISG

The findings reveal that all case study organizations regard the protection of information across the enterprise as an important governance function and are committed to instituting processes to assist integration with IT governance and corporate governance. However, perceptions vary widely as to the locus of ISG in relation to IT governance and corporate governance as shown in Table 3. The results suggest that there is no particular dominant position with respect to the relationship of ISG to IT governance or corporate governance. Rather, emphasis is placed on the need for integration.

1	2	3	4	5	6
Case site	Outsourced IT function	Information Security Governance implicit in IT Governance	Information Security Governance implicit in Corporate Governance only	Separate Information Security Governance Function	Governance Framework Covering Information Security
Energy	✓	✓			✓
Electricity	✓	✓			✓
Bank		✓			✓
Electrical	✓		✓		
Water	✓		✓		
Start-up	✓		✓		
Retail Gas	✓		v		
Distributor	✓			✓	✓
Healthy				✓	✓
Consultant				✓	✓
Differentiator				✓	
Best Practice Co	✓			✓	✓
Advantage				✓	✓
Virtual	✓			✓	

Table 3: Summary of locus of ISG

4.3.1 Information security governance implicit in IT governance

As shown in Table 3, three organizations, Energy, Electricity and Bank, have subsumed their ISG initiatives within their IT governance activities (column 3), which are in turn overarched by corporate governance for different contextually based reasons. For example, Energy, a State owned corporation, is a major electricity generating corporation in Australia, involved in competitive trading of electricity in the National Electricity Market (NEM). Its major business activities are electricity production and energy trading. Within this company, ISG is considered a component of IT governance, which is in turn considered a component of the overall corporate governance. Energy's institutional logic has transformed such that it now views itself as an energy trader rather than merely as an energy generator. This has had important ramifications in respect of additional security requirements, and consequently a key component of the company's IT governance is now a specific ISG Framework.

4.3.2 Information security governance implicit in corporate governance alone

Whilst all cases required ISG to be consistent with the ethos, the principles, and the activities of their overall corporate governance institutions, only four of cases made it implicit within corporate governance alone (column 4). In these cases, no additional specific governance mechanisms are in place to explicitly govern information security. Rather, it is seen as a very central business issue. Notably, all of these organizations have outsourced their IT function.

For example, in the case of Electrical, protecting information across the enterprise is regarded as an important part of the IT strategy. This company is a State-owned electricity distribution and retail company. The company's recent entry to the National Electricity Market (NEM) has caused it to re-think its governance structure and to reassess which committees are required to cope with its entry into the national market. The profile of IT within the company has also been elevated due to its recent entry to the NEM, and the associated major system changes to allow energy trading. No separate IT governance initiatives exist within the company, and there are no separate IT governance or ISG structures. According to a non-executive director, such governance is taken for granted and completely institutionalized across the organization within the overall corporate governance risk management process.

In comparison, Start-up is a relatively new company still in the early stages of development. The company's main activities are to explore and develop coal-bed methane gas fields and to produce and sell gas. Given its early development phase, it has very basic IT requirements. However, its ongoing connectivity to two major gas companies, and intellectual property associated with its unique geological and geophysical information necessitates that high IT security levels are maintained. At Board level, the company has a broad corporate governance focus, rather than an IT governance or ISG view specifically.

4.3.3 Separate information security governance function

Half of the case organizations have elected to govern information security through separate, nominated ISG functions, which are congruent with the respective IT governance and corporate governance initiatives within these organizations. They represent a mix of private and State organizations and vary considerably in size. Thus, as seen in column 5 of Table 3, half of the sample perceive ISG as a separate function in its own right, and five of these seven organizations, Distributor, Healthy, Consultant, Best Practice Co and Advantage, have instituted specific governance frameworks covering the protection of IT and information assets, although these are not ISG frameworks per se, as discussed further below. Two of the companies, Advantage and Differentiator, regard ISG as a strategic differentiator.

4.3.4 Governance framework covering information security

Eight of the 14 case organizations (column 6) have a specific governance framework of some kind to govern information security initiatives, whether the organizations undertake ISG separately in its own right, or as part of wider governance programs. These overarching frameworks were found to engage all organizational and operational processes and participants relevant to information security. For example, Energy governs information security via its IT Governance Framework. Electricity governs information security via a broad governance framework comprising a multitude of IT, compliance and risk management strategies and policies.

In only four of the cases, does an actual overarching ISG framework constitute the cornerstone of ISG. For example, Consultant, a global consulting firm in the financial sector, has in place an IT Security Framework, IT Strategy and IT Security Policy that underpin its ISG efforts. Advantage undertakes ISG via its IT Governance Model, Data

Networking and Hosting Centre Strategies, and IT Security Policy and Strategy. Healthy, a mutual organization that provides health insurance cover to about 2 million Australians, governs information security through an IT Security Governance Framework, which comprises an IT Security Policy, IT Security Procedures, IT Security Guidelines, a Password Policy, and an IT Security Tolerance Level.

The findings reveal different orientations (for e.g. risk management emphasis versus a security focus) and variations in the extent to which ISG is framed as a part of or separate to IT and corporate governance. This highlights how the confluence of multiple institutional forces and technical contexts are shaping heterogeneous forms of ISG.

5 Discussion and implications for future work

This study set out to examine how ISG arrangements were shaped and framed in critical infrastructure organizations in Australia through multiple case studies. ISG was observed as a socio-technical, emergent and situated practice, shaped by the context in which it was located.

5.1 Heterogeneous and malleable arrangements of ISG

The study paints a picture of diverse ISG approaches in the field and shows that ISG arrangements vary widely, despite the evidence of some isomorphism. Conformance and performance objectives for ISG were not found to be universal triggers for decision makers but institutionally contingent. This suggests that the confluence of multiple institutional forces across organizations (e.g. intra-organizational relations), fields (for e.g. critical infrastructure), industries (e.g. energy, water, ICT) and countries (e.g. BS 7799 and AS/NZS 17799 now 27001/27002) may result in variation and heterogeneity rather than homogeneous arrangements of ISG. For example, the protection of information was a core competency of Advantage and Differentiator and viewed as a strategic differentiator in contrast to the remaining cases. Further research is required to gain a deeper understanding of the mix of defensive, protective and enabling foci adopted in practice. In addition, an examination of the events leading up to and processes involved in the institutionalization and de-institutionalization of ISG is needed to progress understanding of socio-technical change surrounding ISG in organizations.

5.2 Multiplicity of beliefs, norms and social logics in ISG

At the field level organizations were formed around the issue of critical infrastructure, as well as in some cases, but not all, similar products and markets. However, ISG in each case organization was found to be a mix of laws, regulations, material practices and strategic imperatives. Hence a multiplicity of cultural beliefs, norms and social logics were found to be at play. These findings support claims in the institutional literature (see for e.g. [Schneiberg & Clemens 2006]) of how fragmented fields can subject organizations to multiple, competing and contradictory logics. Connecting the activities of people and organizations that are informed by and embedded in these multiple logics requires further research.

5.3 Institutional possibilities and extended governance

Whilst the board members and senior level management have leading roles, the findings point to other significant actors such as outsourcing partners and lower level management. The ownership of ISG was not necessarily based on single autonomous organizations. Rather, ISG appeared to be accomplished by interactions and multilateral relationships within and across organizational boundaries. This suggests that single organizations may not be equipped to deal with the complexity associated with ISG requiring networked type governance arrangements with shared accountabilities. Hence attention needs to be directed towards not only structures but also the actions of individuals engaged in steering ISG. Further, the role of professional agents, standard setters and third party providers may provide insights into the emergence of inter-organizational structures and political processes in developing governance arrangements and further progress the concept of institutional entrepreneurship.

5.4 Need for an information centric view

The protection of the information asset itself was identified as a core competency and strategic imperative in both the Advantage and Differentiator cases. Whilst it is commonly accepted that the goal of information security is to protect information assets, there is an assumption that these assets are readily identified and "there is an accepted understanding of what it means to protect" [ITGI 2008: 29]. Locating and identifying information assets, assigning value to these assets and the classification of information assets as to their criticality and sensitivity is recognized in practice as both a "daunting" yet necessary task for ISG to be "effective and relevant" [ibid: 30].

We argue that while there has been a shift in perspective from a technology-centric to a socio-organizational view, there is still significant ambiguity with regard to the concept of information itself and call for an information centric view. Further, an information centric view would not only view information as an object of security but also as an instrument in security; recognized as a critical element in enterprise security intelligence enablement (ESI) [Felman 2010]. Hence more attention needs to be directed towards exploring the interdisciplinary terrain of information protection and probing theoretical ambiguities, to clarify and advance current thinking.

The theoretical, and analytical perspective adopted in this paper provides a valuable lens in which to examine ISG. The extended theoretical view offered assisted in developing a richer theory, which revealed not only the complexity in making information security governable but also the problematic nature of how it is governed. We hope that the analysis presented in this paper may serve to stimulate further interest in ISG and the protection of information more broadly.

References

AGD (2010) Critical infrastructure Resilience Strategy. Australian Government Attorney General's Department.

Allen, J.H., & Westby, J.R. (2007). Governing for Enterprise Security (GES) Implementation Guide Article 1: Characteristics of Effective Security

Governance. The Software Engineering Institute, CERT® Carnegie Mellon University, PA.

Allen, J.H. (2005). Governing for Enterprise Security Technical Note CMU/SEI-2005-TN-023. The Software Engineering Institute, CERT® Carnegie Mellon University, PA.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. Logistics Information Management, 15(5), 337-346.

Caralli, R.A. (2004). Managing for Enterprise Security Technical Note: CMU/SEI-2004-TN-046. The Software Engineering Institute, Carnegie Mellon University.

Deloitte Touche Tohmatsu (DTT). (2007). Global Security Survey The shifting security paradigm. DTT, USA

Dhillon, G., (2007). Principles of Information Systems Security: text and cases. New York: John Wiley and Sons.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16, 293-314.

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review, 45(1), 67-87.

Ernst & Young (E&Y). (2009). Outpacing change: Ernst & Young's 12th annual global information security survey.

Felman, J. (2010). Prepare for the Emergence of Enterprise Security Intelligence. Gartner Research ID Number: G00201051.

Griffith, T., & Dougherty, D.J. (2002). Beyond socio-technical systems: introduction to the special issue. Journal of Engineering and Technology Management, 19, 205-216.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. Journal of Strategic Information Systems, 16, 153-172.

IT Governance Institute (ITGI). (2011). Global Status Report on the Governance of IT (GEIT)

IT Governance Institute (ITGI). (2008). Information Security Governance: Guidance for Information Security Managers.

IT Governance Institute (ITGI). (2006). Board briefing on IT governance, 2nd Edition. ITGI Rolling Meadows, IL USA.

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. Information Management & Computer Security, 14(5), 402-415.

Love, P., Reinhard, H., Schwab, A.J., & Spafford, G. (2010). Global Technology Audit Guide (GTAG®)15 Information Security Governance, Institute of Internal Auditors, USA.

McFadzean, E., Ezingeard, J-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, 31(5), 622-650.

Miles, M.B. & Huberman, A.M. (1994). An Expanded Sourcebook Qualitative Data Analysis 2nd Edition. Thousand Oaks, California: SAGE Publications, Inc.

Orlikowski, W., & Barley, S. (2001). Technology and institutions: What can research on information technology and research on organizations learn from each other? MIS Quarterly, 25(2), 145-165.

Pinch, T. (2008). Technology and institutions: living in a material world. Theory and Society, 37, 461-483.

Schneiberg, M., & Clemens, E. (2006). The typical tools for the job: Research strategies in institutional analysis. Sociological Theory, 24(3), 195-227.

Siponen, M.T., & Willison, R. (2007). A critical assessment of IS Security research between 1990-2004. In H. Österle, J. Schelp & R. Winter (Eds.), Proceedings of the 15th European Conference on Information Systems (pp.1551-1559), St. Gallen, Switzerland.

Siponen, M.T. (2006). Information Security Standards Focus on the Existence of Process, Not its Content. Communications of the ACM, 49(8), 97-100.

Straub, D.W., Goodman, S., & Baskerville, R.L. (2008). Framing the information security process in modern society. In D.W. Straub, S. Goodman & RL Baskerville (Eds.), Information security policies, processes and practices (pp. 5-12). Armonk New York: M E Sharpe, Inc.

Thomson, K-L., & Von Solms, R. (2005). Information security obedience: a definition. Computers & Security, 24(1), 69-75.

Thornton, P.H., & Ocasio, W. (2008). Institutional logic. In R. Greenwood, C. Oliver, K. Sahlin & R. Suddaby (Eds.). The SAGE Handbook of Organizational Institutionalism (pp.99-129). London. SAGE.

Von Solms, B. (2005). Information security governance: COBIT or ISO 17799 or both? Computers & Security, 24, 99-104.