Association for Information Systems
AIS Electronic Library (AISeL)

BLED 2010 Proceedings | BLED Proceedings

2010

Managing Information Risks and Protecting Information Assets in a Web 2.0 Era

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

Susan P. Williams
Institute for Information Systems Research, University of Koblenz-Landau, williams@uni-koblenz.de

23rd Bled eConference
eTrust:
Implications for the Individual, Enterprises and Society
June 20 - 23, 2010; Bled, Slovenia

Managing Information Risks and Protecting Information Assets in a Web 2.0 era

Catherine A. Hardy

Discipline of Business Information Systems, University of Sydney, Australia

catherine.hardy@sydney.edu.au

Susan P. Williams

Institute for Information Systems Research, University of Koblenz-Landau, Germany

williams@uni-koblenz.de

Abstract

The growth in volume of digital information arising from business activities presents organisations with the increasingly difficult challenge of protecting their information assets. Failure to protect such information opens up a range of new business risks. The increase in externally hosted services and social networking tools also adds a new layer of complication to achieving information protection. Prior research has recognised the need for a socio-organisational view of information protection, shifting the emphasis from a narrowly defined technical concern to an enterprise-wide, business-led responsibility encompassing strategic and governance issues. We argue that this shift is important but not enough and that greater attention should be given to understanding the nature and complexities of digital business information. In this paper we examine the extent to which existing frameworks for information protection are structured to account for changes in the information environment. Our findings indicate that whilst these frameworks address the need to adopt a broader social and organisational perspective there remain a number of significant limitations in terms of the way the information is treated. To address these limitations we propose a more co-ordinated and information-centric approach to information protection.

Keywords: information protection frameworks, information risks, Web 2.0

1 Introduction

Recent years have witnessed massive growth in digital information. It is estimated that in 2007 information created, captured, or replicated in digital form exceeded 281 exabytes. In 2011 the volume of digital information produced will be close to 1,800 exabytes, ten times that produced in 2006 (Gantz et al 2008).

Alongside the growth in volume are increases in the types, forms and formats of information and the range of systems used to create, manage and protect digital

information. It is also estimated that unstructured data already accounts for more than 80% of all information (Gantz et al 2007).

Organisations are facing the challenge of protecting their information assets within a complex and changing environment. They must protect multiple forms of information (e.g. traditional documents, text messages, video, email, audio, RFID) within diverse systems and technologies (e.g. databases, document, records and content management systems, social networking tools, mashups). Increasingly these systems are being externally hosted (e.g. Software as a Service (SaaS), cloud computing) and often beyond the direct control of the organisation. For example when information is published and stored on employees' personal blogs, Facebook, Twitter and other social networking sites. The value of Web 2.0 and Enterprise 2.0 tools and media to organisations is increasingly being recognised (Edwards 2009, Buhse and Stamer 2008, Cook 2008) however alongside this potential value come additional business risks (Short 2008, Mar 2010).

Organisations must also comply with diverse legal and regulatory mandates at national and international levels. It is estimated that 20% of digital information is subject to some form of legal or regulatory compliance, requiring formal policies and strategies for its effective protection and retention (Gantz et al 2007). There is growing recognition that organisations need to focus greater attention on e-compliance and the management of risks arising in a digital environment (Gasser & Hauesermann 2007). Further, there are growing concerns around the capability of organisations to comply with legislation relating to privacy, data protection and legal discovery. A recent survey of senior IT executives identified that one in three organisations have had the experience of being unable to recover files from backup and a similar proportion could not easily produce emails sent and received only 18 months ago to comply with a legal discovery audit (Hitachi 2009).

These changes in the information environment pose major challenges for organisations. One of the key challenges organisations face is that of reconciling the fact that on the one hand information is a source of business value, to be re-used and re-purposed, shared and distributed in flexible ways with the management of information risks and the retention of business information as evidence.

In this paper we focus on the risk side of digital information management and consider organisations' information protection capability. Failure to adequately manage and protect digital information assets exposes an organisation to significant business and information risks including:

> *Continuity risk*—the risk associated with the availability of information and its backup and recovery;
>
> *Compliance risk*—the risk of not being able to provide the required information to comply with relevant laws and regulations, including for example, privacy, data protection and legal discovery legislation;
>
> *Auditability risk*—the risk of not being able to verify and obtain assurance about the integrity of information due to incomplete documentation;
>
> *Reputational risk*—the reputational damage arising from accidental or deliberate destruction of documents or the release of confidential or personal information;

Intellectual Property risk—loss of rights in literary and artistic creations or the loss of such proprietary information itself.

Content risk—the loss of control of information assets as they are re-used, re-purposed and re-combined.

Our aim in this paper is to investigate the extent to which current frameworks for information protection encompass the changes we are witnessing in the information environment and described above. Specifically our objectives are 1) to identify the scope of the different frameworks and the ways (if any) that the socio-organisational and inter-organisational aspects of information protection are embedded within existing frameworks and 2) to understand how the information itself is represented in such frameworks.

The paper is organised as follows. In the next section we provide a brief review of the information protection imperative both as an issue for organisations and in the context of recent developments in scholarly research literature. This is then followed in Section 3 by an analysis of integrated frameworks for information protection. Our aim in this section is to provide a synthesis and critique of the range and scope of existing frameworks. In Section 4 we discuss the implications of our findings and present the requirements for an expanded framework for enterprise information protection.

2 Background and context

Protecting the confidentiality, integrity and availability of information assets is a significant business challenge. Information protection failures may result in information loss, serious system disruptions, business continuity failures and compliance breaches; increasing strategic and reputational risks through loss of valuable intellectual property, customer trust and competitive opportunities. The changing technology environment introduces new ways for information to be shared and with them come new information risks. Organisations that protect and leverage their information assets through effective information policies will be in a stronger position to manage future business risks and realise business value. Recent reviews of research in the field of information security identify a number of limitations of current research and call for a reassessment of the research agenda. Limitations identified include: concerns that the field of information security lacks a focus on socio-organisational issues (Dhillon & Backhouse 2001; Siponen & Willison 2007), poor use of research theory and methods (Björck 2004) and a shortage of empirical studies (Siponen and Oinas-Kukkonen 2007).

Recent high profile examples of information protection failure illustrate that achieving a sustainable protection capability continues to present a major challenge for organisations in both the private and public sectors (O'Toole 2007, Walters 2007, ICO 2007). These recent examples of information protection failure occurred not because of poorly designed information security technologies but as a consequence of the way those technologies were used and integrated with broader organisational information protection policies and communicated across the organisation. A recent survey found that 79% of participants cited the human factor (e.g. employees, business partner, suppliers) as the cause of information security failures and that despite business executives becoming more aware of IT security issues, support for a solution still predominantly lies with the IT department (Deloitte 2007).

Organisations are actively pursuing widely accepted best practice exemplified in standards and frameworks such as AS/NZS ISO/IEC 27001/27002:2006 Information Security Standard, IT Governance Institute (ITGI) Control Objectives for Information and related Technologies (COBIT) 4.1, and the UK Office of Government Commerce (OGC's) Information Technology Infrastructure Library (ITIL).

However, whilst work is underway to map different standards and frameworks to provide a broader picture, the focus remains on narrow forms of information, systems and types of security (ITCI 2007:p.2). There is also limited understanding of how the objectives of these standards are actually achieved in organisations (Siponen 2006).

A limitation of earlier research is that most attention is focused on the technical and risk management aspects of information security. There is now growing recognition that whilst such technical solutions are necessary they are not sufficient and a change in perspective is required (Baskerville & Siponen 2002; Siponen 2005; Dhillon 2007). To address this limitation recent work has begun to expand the scope of information security research, placing greater emphasis on strategic and governance issues (cf. Caralli 2004; Allen and Westby 2007). Focus has moved 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 and protecting information assets (ITGI 2006; ITCI 2007).

3 Analysis and critique of integrated frameworks for information protection

In this section we present the findings of our critial analysis of integrated frameworks for information protection.

3.1 Identifying the frameworks

We based our analysis strategy on the guidelines suggested by Webster and Watson (2002 p. xvi). We identified relevant frameworks by undertaking the following steps:

- keyword search using the Business Source Premier, ProQuest5000, IEEE Xplore and ACM Digital Library databases;
- examination of research review papers (*cf.* Dhillon & Backhouse 2001; Siponen 2005; Siponen & Willison 2007; Siponen & Oinas-Kukkonen 2007);
- review of relevant books (*cf.* van Bon & Verheijen 2006; Dhillon 2007; Straub et al. 2008c); and a
- review of publications of key professional groups active in the area of information protection (*cf.* Carnegie Mellon Computer Emergency Response Team http://www.cert.org/work/organizational_security.html; IT Governance Institute http://www.itgi.org/; Information Systems & Control Association http://www.isaca.org/ Standards Australia http://www.standards.org.au/)

Forward and backward citation analysis of the retrieved publications was conducted to identify additional relevant frameworks. The ISI Web of Knowledge was also used to identify publications that cited the frameworks identified from the review process for the purpose of gauging when the search had reached saturation and to ensure we were

working with the most up to date version. Our search resulted in the selection of nine key frameworks.

3.2 Review of frameworks

An analysis of the nine key candidate frameworks was completed. Table 1 summarises the extent to which they 1) encapsulate a socio-organisational view (elements, scope of application and context) and 2) assess how information is represented (information view). For example, does the framework explicitly specify the nature and forms of information to be protected? does it take a particular view of information (e.g. data protection view)? or is the concept of information black-boxed and taken for granted?

<table>
<tr><td colspan="3">i. Hong et al. (2003) – An integrated system theory of information security management
Focus: Integrated strategic framework for information security management (ISM)</td></tr>
<tr><td colspan="3">Socio-organisational view</td></tr>
<tr><td>Elements</td><td>Scope of Application</td><td>Context</td></tr>
<tr><td>1. Organisational structures √
2. Stakeholders
3. Processes
4. Technology
5. Environment √</td><td>6.Governance
7. Risk management √
8. Control & assurance √
9. Security management √
10. IT management
11. Other mgt activities √
12. Legal & Compliance
13. Strategy/Policy √
14. Inter-organisational
15. Capability</td><td>Internal & external environment - nature of intra & inter organisational relationships unexamined.
Functional emphasis for integrating information security.
Single goal to align information security with organisational objectives.</td></tr>
<tr><td colspan="3">Information view</td></tr>
<tr><td colspan="3">Information management & techniques as managerial activities.</td></tr>
</table>

II. ITGI (2006) – Information security governance **Focus: Governance of information security**				
Socio-organisational view				
Elements		**Scope of Application**		**Context**
1. Organisational structures	√	6.Governance	√	Internal & external stakeholders- nature of intra & inter organisational relationships unexamined. Process emphasis on integration-management processes (multi level) & assurance efforts. Multiple goals: strategic alignment, risk mgt, resource mgt, performance mgt & value delivery. Capability view – assess information security governance maturity/levels
2. Stakeholders	√	7. Risk management	√	
3. Processes	√	8. Control & assurance	√	
4. Technology	√	9. Security management	√	
5. Environment	√	10. IT management	√	
		11. Other mgt activities	√	
		12. Legal & Compliance		
		13. Strategy/Policy	√	
		14. Inter-organisational		
		15. Capability	√	
Information view				
Protecting information assets distinct from information technology.				

III. Karyda et al. (2006) – A framework for outsourcing IS/IT security services **Focus: Major technical, organisational and legal issues pertaining to outsourcing**				
Socio-organisational view				
Elements		**Scope of Application**		**Context**
1. Organisational structures	√	6.Governance		Environment – internal (eg. culture) & external (laws). Inter-organisational emphasis on business partnerships but nature of not examined. Functional emphasis on integration. Single goal – formulating IS/IT security outsourcing strategy. Capability– core competencies.
2. Stakeholders		7. Risk management		
3. Processes		8. Control & assurance	√	
4. Technology	√	9. Security management		
5. Environment	√	10. IT management	√	
		11. Other mgt activities	√	
		12. Legal & Compliance	√	
		13. Strategy/Policy	√	
		14. Inter-organisational	√	
		15. Capability	√	
Information view				
Data protection – specifically privacy & security.				

IV. AS/NZS ISO/IEC 27002 (2006) Information technology security techniques – code of practice for information security management
Focus: Information security management

Socio-organisational view

Elements		Scope of Application		Context
1. Organisational structures	√	6.Governance		Environment – internal (eg.roles & responsibilities) & external (laws).
2. Stakeholders	√	7. Risk management	√	Nature of inter-organisational focused on identifying risks related to external parties, customers & third parties.
3. Processes	√	8. Control & assurance	√	Functional emphasis on integration.
4. Technology	√	9. Security management	√	Multiple goals – integrity, availability, confidentiality
5. Environment	√	10. IT management	√	
		11. Other mgt activities	√	
		12. Legal & Compliance	√	
		13. Strategy/Policy	√	
		14. Inter-organisational	√	
		15. Capability		

Information view

Control and legal emphasis relating to: Data protection and privacy of personal information; protection of organisational records; and intellectual property rights. Inventory of information assets and classifications.

V. ITGI COBIT© Security Baseline (2007) – An information security survival kit
Focus: IT governance and control

Socio-organisational view

Elements		Scope of Application		Context
1. Organisational structures	√	6.Governance	√	Environment – internal (eg.roles & responsibilities) & external (laws).
2. Stakeholders	√	7. Risk management	√	Nature of inter-organisational focused on controls over business transactions and information exchanges between enterprises, customers, suppliers, partners & regulators.
3. Processes	√	8. Control & assurance	√	Functional emphasis on integration.
4. Technology	√	9. Security management	√	Multiple goals – availability, confidentiality, integrity, trust (authenticity & non-repudiation)
5. Environment	√	10. IT management	√	Capability – maturity/levels
		11. Other mgt activities	√	
		12. Legal & Compliance	√	
		13. Strategy/Policy	√	
		14. Inter-organisational	√	
		15. Capability	√	

Information view

Information recorded on, processed by, stored in, shared by, transmitted from or retrieved from any medium.

VI. daVeiga & Eloff (2007) – An Information Security Framework **Focus: Governance**				
Socio-organisational view				
Elements		**Scope of Application**		**Context**
1. Organisational structures	√	6.Governance	√	Environment – internal (eg.roles & responsibilities) & external (laws).
2. Stakeholders	√	7. Risk management	√	Nature of inter-organisational relationship not examined.
3. Processes	√	8. Control & assurance	√	Functional emphasis on integration.
4. Technology	√	9. Security management	√	Goals – governing information security holistically
5. Environment	√	10. IT management	√	Change management incorporated
		11. Other mgt activities	√	
		12. Legal & Compliance	√	
		13. Strategy/Policy	√	
		14. Inter-organisational		
		15. Capability		
Information view				
Information asset mgt– inventories, classification & labelling				

VII. CERT® Resiliency Engineering Framework (2008) **Focus: Enterprise wide and capability**				
Socio-organisational view				
Elements		**Scope of Application**		**Context**
1. Organisational structures	√	6.Governance	√	Environment – internal (eg. HR mgt) & external (supplier mgt). Inter-organisational viewed as external dependency operational capability.
2. Stakeholders	√	7. Risk management	√	Capability emphasis on integration.
3. Processes	√	8. Control & assurance	√	Objectives centred around resiliency.
4. Technology	√	9. Security management	√	Capability areas and levels.
5. Environment	√	10. IT management	√	
		11. Other mgt activities	√	
		12. Legal & Compliance	√	
		13. Strategy/Policy	√	
		14. Inter-organisational	√	
		15. Capability	√	
Information view				
Knowledge & information mgt – 1 of 21 capability areas in resiliency mgt. Information assets: *Forms* (eg.paper, CDs, digital *Location* (portable media, servers) *Resiliency* (how used & value) *Use* and *Classification.* Rules, laws etc. information is subjected to.				

VIII. van Bon et al./ITIL v3 (2008) - Service Design based on ITIL® v3, A Management Guide. Focus: Business strategy – IT service delivery					
Socio-organisational view					
Elements		**Scope of Application**		**Context**	
1. Organisational structures	√	6.Governance		Environment – internal & external (suppliers, partners).	
2. Stakeholders	√	7. Risk management	√	Functional emphasis on integration.	
3. Processes	√	8. Control & assurance	√	Objective centred around service delivery	
4. Technology	√	9. Security management	√		
5. Environment	√	10. IT management	√		
		11. Other mgt activities	√		
		12. Legal & Compliance	√		
		13. Strategy/Policy	√		
		14. Inter-organisational	√		
		15. Capability			
Information view					
Information technology management focus					

IX. ISACA (2009) Business model for information security Focus: Enterprise wide security and capability					
Socio-organisational view					
Elements		**Scope of Application**		**Context**	
1. Organisational structures	√	6.Governance	√	Environment – internal & external. Nature of inter-organisational relationship not examined.	
2. Stakeholders	√	7. Risk management	√	Cultural emphasis on integration.	
3. Processes	√	8. Control & assurance	√	Objective centred around creating a security culture.	
4. Technology	√	9. Security management	√	Capability – focus/levels (eg. communication)	
5. Environment	√	10. IT management	√		
		11. Other mgt activities	√		
		12. Legal & Compliance	√		
		13. Strategy/Policy	√		
		14. Inter-organisational	√		
		15. Capability	√		
Information view					
Protecting information					

Table 1 – Review of key information protection frameworks

Our review of the integrated information protection frameworks revealed that socio-organisational aspects are now firmly embedded within existing frameworks, although they are conceptualised and employed differently. Inter-organisational and to a greater extent representations of information itself were found to be much less insightful for

addressing the diverse and changing nature of the information environment. Following is a synthesis of our findings.

The integrated functional socio-organisational view

Integration of the elements and applications of the socio-organisational view was mostly based on functions and organisational goals. In this context, organisations and information systems are viewed as concrete entities. Whilst the value of such models is evident, they provide limited insights into the complex dynamics of diverse intra- and inter-organisational processes. In the current information age, organisational structures are changing from relatively stable hierarchical structures to more loosely coupled and networked arrangements extending beyond organisational boundaries. Further, as Web 2.0 technologies dynamically interact within formal and informal environments, the importance of understanding behaviours and interactions around dynamic social groupings is of increasing importance.

Strategy, policy and risk focus

Common to all frameworks was the importance placed on the concepts of strategy, policy and risk. However, limited attention was given to the interests and values of different stakeholders in giving meaning to risk, the contexts in which policy debates take place, and strategy setting processes. Of the nine frameworks examined, five, namely, ISACA (2009), CERT® (2008) CobiT© Security Baseline (2007), Da Veiga and Eloff (2007) and ITGI (2006) made explicit reference to providing an holistic approach for addressing business and strategic objectives alongside, risk and conformance objectives. Further, whilst Karyda et al. (2006) focused on factors pertaining to strategies for the outsourcing of IS/IT security services, their conceptualisation of legal issues is unique to the other frameworks. The framework highlights the range and complexity of issues in terms of defining the applicable law (such as privacy, intellectual property and contract law) as well as the jurisdictions under which the organisation and provider operate (p. 409). These views are reinforced by Turle (2009, p.25) for example who states that protecting information "is just as much about employment law, property law and contract law as it is about data protection law" requiring consideration of different legal frameworks. Explicit consideration of Web 2.0 and Enterprise 2.0 risks and policies is currently absent from these frameworks.

The information blackbox

The CERT® (2008) had the most detailed view of information itself, as information management is a key capability area in the resiliency framework. The remaining frameworks blackbox the concept as, for example, an organisational asset or distinct from data or IT. This confirms Straub et al.'s (2008a p. 6) views that notwithstanding "information is a managerial and organizational tool … [it] "has not been subject to the same intense scrutiny as have security technologies." The unprecedented levels of collaboration, exchange of information and user generated content offered by Web 2.0 platforms requires a shift in the protection emphasis from guarding infrastructure to a focus on the integrity of information as it is used and edited and the context of its use. This itself will require greater attention to the construction of quality risk intelligence.

4 Future directions: a coordinated and information-centric view of information protection

As we outlined in the introduction, the changing information environment is presenting organisations with new forms of information and new methods of creating, storing and protecting that information. This change has accelerated with the increasing availability of Web 2.0 and Enterprise 2.0 tools and methods for social networking and content aggregation.

Our review of current frameworks for information protection identifies limitations in the way information perspectives are treated. Whilst the frameworks may be adequate for handling and protecting traditional forms of business information such as databases and structured document management systems, they appear much less well-suited to handling the increasingly complex, unstructured, re-used and re-purposed information found in organisations today. The frameworks are also largely silent on the matter of inter-organisationally shared information and the growing volumes of personally created information residing in mobile devices etc. The information risks created through the use of social networking tools and new media are also not visible in existing frameworks. A recent survey of how organisations are using Web 2.0 indicates that of the 2,847 executives surveyed nearly three-quarters plan to maintain or increase investments in Web 2.0 technologies (McKinsey 2007). It is essential that these important sources and destinations of business information are accommodated in future approaches to information protection,

Looking forward information protection requires a stronger focus on information and the locus of creation, use and control of all information assets is required. This requires greater emphasis on information mapping and on understanding who is creating what information, on behalf of whom and for what purpose. Traditional information audit and information mapping approaches (e.g. Henczel 2001; Horton 1998) go some way to assisting in this process, however further work is necessary to extend these methods to account for a more complex information and technology environment. These should also accommodate information about the protection of information across its entire lifecycle.

Also in terms of risk mapping, the risk management area in most frameworks is concerned with identifying and analyzing the risks – taking a prescriptive stance using it as a technique to establish controls. Risk mapping methods also require extension to provide practical guidance at the point of creation and use. This view is supported by Baskerville (1991) (cited in Dhillon & Backhouse 2001:140-141) stating that the predictiveness of risk analysis is of less value than its “real usefulness” which “lies in it being an effective communication tool, especially between security and management professionals.”

A wide range of stakeholders are involved in information protection including specialists in IT and security, legal and compliance, records management etc. The everday business user currently has little role to play even though they are often the creator and custodians of their own and their business unit's information assets. Gantz et al (2007) estimated that “three quarters of organizational information lies in the domain of the data center, another one quarter out in other departments. […] though, the responsibility for security, privacy protection, and compliance with legal requirements

regarding data retention, is almost 100% centralized". This raises the question of the role of the business information expert, the person using and managing that information every day. Not only do these users require training and awareness about their organisations information protection policies and practices they may also have a role to play in participatory governance. These are areas for further investigation.

References

Allen JH & Westby JR. (2007). Characteristics of Effective Security Governance. CERT Software Engineering Institute Report, Carnegie Mellon University. http://www.cert.org/governance/ges.html

AS/NZS ISO/IEC 27002:2006 (2006). Information technology – Security techniques - Code of practice for information security management, Standards Australia.

Baskerville R & Siponen MT. (2002) An information security meta-policy for emergent organisations. Logistics Information Management, Vol. 15(5/6) 337-346.

Björk F. (2004). Institutional theory: A new perspective for research into IS/IT security in organizations. Proceedings of the 37th Hawaii International Conference on System Sciences, pp 1-5.

Buhser, W & Stamer, S. (2008). The Art of Letting Go. Enterprise 2.0. New York: iUniverse.

Caralli RA. (2004). Managing for Enterprise Security. Technical Note: CMU/SEI-2004-TN-046. Carnegie Mellon University: Pittsburg. http://www.cert.org/archive/pdf/04tn046.pdf

CERT®, (2008). CERT® Resiliency Engineering Framework, Preview version, v0.95R, Software Engineering Institute, Carnegie Mellon. http://www.cert.org/archive/pdf/REFv0.95R_outline.pdf.

Cook, C. (2008) Enterprise 2.0 How Social Software Will Change the Future of Work. Farnham: Gower.

Da Veiga A & Eloff JHP. (2007). An Information Security Framework, Information Systems Management, Vol. 24, 361-372.

Deloitte Touche Tohmatsu. (2007) 2007 Global Security Survey, The shifting security paradigm. http://www.deloitte.com/dtt/research/0,1002,sid=1013&cid=170582,00.html

Dhillon G. (2007). Principles of information systems security, John Wiley & Sons: United States of America.

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

Edwards R. (2009). Collaboration 2.0. White Paper. Ovum Butler Group.

Gantz JF, Chute C, Schlichting et al (2007). The expanding digital universe. IDC White Paper.

Gantz JF, Chute C, Manfrediz A, et al. (2008). The diverse and exploding digital universe. IDC White Paper

Gasser U & Haeusermann DM. (2007) E-compliance: Towards a roadmap for effective risk management. Research publication No 2007-3. Harvard Law School.

Henczel S. (2001) The information audit: a practical guide. KG Saur.

Hitachi (2009). The Great Information Glut. Hitachi Data Systems. http://www.hds.com/assets/pdf/apac-site/anz/research-report-great-information-glut.pdf

Hong K-S, Chi Y-P, Chao LR, Tang JH. (2003) An integrated system theory of information security management, Information Management & Computer Security. Vol.11(5), 243-248.

Horton FW (1998). Mapping corporate information resources. International Journal of Information Management. Vol 8, 245-254.

ICO (2007) Confidential details lost by Revenue and Customs. ICO Statement. 2007-11-20. http://www.ico.gov.uk/upload/documents/pressreleases/2007/personal_details_lost_by_hmrc_201107003.pdf

ISACA (2009) An introduction to the business model for information security. ISACA Rolling Meadows, USA. http://www.isaca.org/Template.cfm?Section=Research2&CONTENTID=47532&TEMPLATE=/ContentManagement/ContentDisplay.cfm

IT Compliance Institute (ITCI). (2007) Information Security & GRC Research Report. http://www.itcinstitute.com/

IT Governance Institute (ITGI). (2006). Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Ed. http://www.itgi.org/Template_ITGI.cfm?Template=/Search/ITGISearchDisplay.cfm

IT Governance Institute (ITGI). (2007). CobiT Security Baseline, An information security survival kit. IT Governance Institute. http://www.isaca.org/Template.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=36388&MicrositeID=0

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

McKinsey (2007). How businesses are using Web 2.0: A McKinsey Global Survey. The McKinsey Quarterly.

Mar S. (2010). Friend or For? Internal Auditor. February 2010. 22-23.

O'Toole C. (2007). Tax Office checks security after bungles, The Australian Financial Review, 6th December.

Short J. 92008) Risks in a Web 2.0 World. Risk Management. October 2008. 28-31.

Siponen M. (2005). An analysis of the traditional IS security approaches: implications for research and practice, European Journal of Information Systems, Vol 14, 303-315.

Siponen MT. (2006). Information security standards focus on the existence of process, not its content, Communications of the ACM, Vol 49(8), 97-100.

Siponen MT & Oinas-Kukkonen H. (2007). A review of information security issues and respective research contributions. The DATA BASE for Advances in Information Systems, Vol 38, (1) 60-80.

Siponen M, Willison R. (2007). A Critical Assessment of IS Security Research between 1990-2004. Fifteenth European Conference on Information Systems, Österle H, Schelp J, Winter R (Editors). 1551-1559, University of St. Gallen, St. Gallen.

Straub DW, Goodman S, Baskerville RL, (2008a). Framing the information security process in modern society, "Information security policies, processes and practices", Straub, D.W., Goodman, S. and Baskerville, R.L., (Editors), M E Sharpe, Armonk New York.

Straub DW, Goodman S & Baskerville RL. (Editors) (2008c). Information security policy, processes and practices, M E Sharpe, Armonk New York.

Turle, M. (2009) Data security: Past, present and future, Computer Law & Security Review, Vol 25, 51-58.

van Bon J & Verheijen T. (Editors) (2006). Frameworks for IT Management, itSMF, Van Haren Publishing, Zaltbommel

van Bon J, de Jong A, Kolthof A, Pieper M, Tjassing R, van der Veen A, & Verheijen T. (2008) Service Design based on ITIL® v3, A Management Guide, Van Haren Publishing, Zaltbommel.

Walters K. (2007). Data security lapse exposes private details. Business Review Weekly June 14-20, 10.

Webster J & Watson RT. (2002). Analyzing the past to prepare for the future: Writing a literature review, MIS Quarterly, Vol 27 (2,) xiii – xxiii.