Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2009

Measuring Information Security Governance Within General Medical Practice

Rachel J. Mahncke
Edith Cowan University

Donald C. McDermid
Edith Cowan University

Patricia A. Williams
Edith Cowan University

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2014
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/9

Measuring Information Security Governance Within General Medical Practice

Rachel J Mahncke, Donald C McDermid & Patricia A H Williams
School of Computer and Security Science
Edith Cowan University

Abstract

Information security is becoming increasingly important within the Australian general medical practice environment as legal and accreditation compliance is being enforced. Using a literature review, approaches to measuring information security governance were analysed for their potential suitability and use within General Practice for the effective protection of confidential information. The models, frameworks and guidelines selected were analysed to evaluate if they were Key Performance Indicator (KPI), or process driven; whether the approach taken was strategic, tactical or operational; and if governance or management assessment tools were presented. To measure information security governance, and be both effective and practical, the approach to be utilised within General Practice would need to function at an operational level and be KPI driven. Eight of the 29 approaches identified, were deemed to be applicable for measuring information security governance within the General Practice environment. However, further analysis indicated that these measurement approaches were either too complex to be directly implemented into General Practice, or collected self-assessment security data rather than actual security measurements. The literature review presented in this paper establishes the need for further research to develop an approach for measuring information security governance within General Practice.

Keywords

Information security, governance, General Practice, medical information security, small business

INTRODUCTION

Australia is in the process of adopting a national approach towards the secure electronic exchange of health information (AHMC, 2008). The contribution of General Practice, as a distinct medical speciality, will be critical to the successful implementation of an interoperable healthcare system (NEHTA, 2006). General Practices provide primary patient care, and as such it is anticipated that they will be involved in a large proportion of the electronic information exchanges within the proposed e-health system (NEHTA, 2006). Protecting confidential electronic health information will require appropriate security measures in regards to technologies, policies, and processes as well as staff that are trained and aware of these security activities (Williams, 2007a). However, information security research conducted by Williams (2008a) within General Practices indicates that security processes could be significantly improved. Therefore, improvements in information security practice within General Practice are required before the exchange of confidential patient information can be realised.

Incorporating information security governance into General Practice is one solution to promote improvement in information security practice. Information security governance is considered to be part of Information and Communication Technologies (ICT) governance (IT Governance Institute, 2007), which itself is a key area of corporate governance (Pironti, 2007). Corporate governance usually comprises of three core elements, that of accountability, transparency and participation (Weill & Ross, 2004), and refers to the way in which a company is "managed, monitored and held accountable to stakeholders for its actions" (Rezaee, 2009, p. 29). Most literature and research in governance is in the context of large organisations with little reference to implementing governance within small businesses, such as General Practices. The World Bank (2002) believes that governance, and by implication information security governance, can be implemented in an organisation of any size, even an organisation consisting of a single person.

An important distinction needs to be drawn between the terms management and governance as these terms are often used interchangeably (de Haes & Van Grembergen (2004); Guldentops, 2004, p.4). Management refers to the traditionally accepted activities of "planning, organising, staffing, leading or directing, and controlling an organisation for the purpose of accomplishing the business objectives" (de Haes & Van Grembergen, 2004). Many areas of information security management can be considered to fall within the scope of governance (ISO 27799, 2008). Governance however, relates to decisions that "define expectations, grant power or verify performance" (de Haes & Van Grembergen (2004). Governance is more concerned with measuring performance, and then based on these results, determining and adjusting the organisations practices to meet future needs (de Haes & Van Grembergen (2004).

Information Security Governance within General Practice

Whilst governance practices are beginning to be adopted in small businesses (Uhlaner & Wright, 2007: Kyereboah-Coleman & Amidu, 2008), there is little evidence of information security governance implementation within small

businesses. Williams' (2008b) Tactical Information Governance Security model – CMM (TIGS-CMM) model was the only information security governance model found that was specifically developed for General Practice businesses. Small General Practices behave quite differently to large organisations predominantly due to not having the same availability of resources, such as financial and time resources. This manifests in many ways, for example it breeds a culture of cost accountability for every financial outlay made. The lack of time and ICT knowledge may also prevent small General Practices from accessing research and applying benchmark information security solutions to their small business needs. Further, General Practices are unlikely to employ dedicated ICT staff within the practice, and so keeping up-to-date on information security practices is an added burden on practices. Therefore, whilst General Practices are aware of information security practices such as those outlined by the General Practice Computing Group's (GPCG) computer security guidelines; they tend to address information security when required to do so by accreditation compliance and Medicare incentive programs.

Further, General Practices do not have the dedicated number of employees or multiple levels of management that exist in larger organisations. Large organisations with a greater number of employees to address information security practices are able to implement robust and complex information security management and governance processes. Yet small General Practices are susceptible to the same threats and vulnerabilities as larger organisations, and still need to meet a minimum standard to protect their confidential information. To further complicate matters, General Practices often outsource their information security processes which raises further questions in regards to what governance processes are in place to monitor how well the outsourced partner follows industry standard security practices.

A major challenge for General Practices is to identify, from the vast number of standards designed for large organisations (for example ISO 27799-2008 2008; NIST 2009; IT Governance Institute 2007), a set of standards and guidelines that are both relevant and practical. This raises questions of who in a practice would have the security skills and knowledge to undertake this review; how should it be structured; what areas should it cover; and what would be a reasonable level of detail to include in such a resource.

This paper presents a discussion on measuring information security governance in relation to some of the challenges therein, and identifies the benefits and relevance of improving security. This is followed by an examination of the literature that contains approaches or concepts of information security governance relevant to General Practice. The purpose of this examination is to identify existing frameworks that could be applied to the General Practice environment, and the themes and issues for future research in this area of application. Finally, the conclusion section summarises the main findings of this discussion.

MEASURING INFORMATION SECURITY GOVERNANCE

The ability to measure governance processes provides the best measure of governance performance (Beveridge, 2008). Practical measurements or assessment of security processes, such as malware statistics, are considered to be the most useful of all security tests. Having metrics provides the necessary quantitative information required to manage information risks and threats (Kabay, 2009; Xenos, 2004). Utilising specific criteria such as Key Performance Indicators (KPI) is a good way of validating that the security procedures implemented by an organisation have been effective (Pironti, 2007). For example, the number of intrusion events may be considered a KPI. The ability to count the number of these events provides a useful measure of information security governance performance (Pironti, 2007). Therefore, implementing governance processes alone, without a method for measuring governance performance, does not provide assurance that the governance processes are effective (Xenos, 2004).

Information security practices can be difficult to measure. Whilst Hinson (2006) argues that it is possible to successfully measure information security, he also acknowledges the difficulties inherent in the measurement process. He cautions against implementing the wrong metrics, measuring the wrong elements, subjectivity, understanding tangible and discrete value outcomes, absolute measurements, the cost of measuring to organisations, the interdependencies between management and measurement, measuring process outcomes and the meaning of numbers (Hinson, 2006). Hinson (2006) advises organisations to focus on the meaning of the outcome for their organisation and its practices, and not to become overly preoccupied by the measurement 'number' outcome. Subjectivity in the measurement outcome can be avoided by correlating the measurement with other related outcomes to confirm that the findings are valid (Hinson, 2006). The aim of measurement therefore, is to improve security practice with objective, repeatable and sustainable measurement practices (Hinson, 2006).

APPROACHES FOR MEASURING GOVERNANCE

A large body of research has focused on information security management and associated governance practices. An extensive search of the literature identified twenty nine research papers which proposed a wide range of approaches for measuring corporate governance, ICT management, ICT governance and information security management and

governance. Assessment tools utilised to measure other forms of governance (such as the extensive research conducted by The World Bank (2002) into political governance and corruption) were not considered for inclusion in this research, as their approaches were considered to be difficult to apply to information security governance. The search results ranged from single academic research papers proposing a wide range of assessment techniques and tools for security management and governance, to key global organisations such as the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST) and the Control Objectives for Information and related Technology (CobiT). These organisations have published extensively in the area of ICT and information security, and use information security measurement techniques that have become best practice industry standards. The models, frameworks and guidelines considered applicable to General Practice have been synthesised in Table 1 to indicate the following column information: Author and/or Organisation Name and Year of publication, whether the assessment tool was Process or KPI driven, whether the assessment tool was aimed at a Strategic, Tactical or Operational level, and the area of application for which the assessment tool was designed.

The twenty nine papers were analysed in two stages. Firstly, each paper was assessed to determine if it was Process or KPI/criteria driven. KPIs define and measure the progress towards organisational goals (Wolcott Group, 2008). KPIs are "significant measures used on its own, or in combination with other KPIs, to monitor how well a business is achieving its quantifiable objectives" (Da Veiga, Martins & Eloff, 2007). Focusing on KPIs will enforce the measurement and execution of information security practice and therefore can be considered to be a criteria driven approach. If the paper presented measurable KPIs or security criteria, such as the percentage of back-up operations that are successful (ISO/IEC 27002), they were detailed as such. Approaches were considered to be process driven if they detailed as a procedure, governance assessment or measurement as a step-by-step process without definitive measurement details for each aspect of the process. Ocasionally papers were assessed as containing both Process and KPI approaches.

Secondly, papers were assessed as to whether they operated and focused the organisation at a strategic, tactical or operational level. The policy-driven strategic level operates at the board and executive levels and deals with broad organisational goals including processes such as reports to stakeholders, strategic vision and allocation of information security resources (ISM3, 2007; Nnolim, 2008). The guidelines-driven tactical level deals with the design and implementation of the allocated resources, and the measures-driven operational level is concerned with the day-to-day execution of security actions such as managing malware protections and the handling of incidents (ISM3, 2007; Nnolim, 2008). Policy however, derived from the strategic level, is the driver for operational level procedures (Williams, 2008a). Policy is derived from legal requirements, professional accreditation and established industry best practice such as those provided by the Royal Australian College of General Practitioners (RACGP) and the General Practice Computing Group (GPCG) (Williams, 2007c). Papers that were graded as strategic or tactical were typically written for large organisations that include many layers of management with large distinct ICT functions and many personnel. The relevance of these approaches to General Practice was considered somewhat limited as small General Practices often do not have ICT staff with the required skill and knowledge to bridge the gap between strategic goals and specific information security practices. Papers assessed as being at the operational level contained specific and detailed security criteria. This level of implementation detail that could be directly applied to General Practices was of specific interest to this research. Occasionally papers were assessed as operating at more than one strategic, tactical or operational level. The predominant operational level has been highlighted in bold in Table 1 below.

Area of Application was determined by the author and included in the table to provide a context for the assessment approach. Eight assessment approaches were considered to be both KPI driven and as operating at an operational level, and therefore possible approaches for measuring information security governance within General Practice. The approaches listed below in alphabetical order are ECUCAUSE (2004), Eibl, Von Solms & Schubert (2006), ISO/IEC 27002 (2006), Kruger & Kearney (2006), NIST (2008), Pironti (2007), Weill & Ross (2004), and the Wolcott Group (2008). The following section evaluates these eight approaches.

Table 1 - Summary of Approaches for Measuring Governance

AUTHOR/S/ORGANISATION (YEAR)	PROCESS OR KPIs (Criteria) DRIVEN	STRATEGIC, TACTICAL OR OPERATIONAL	AREA OF APPLICATION
Beveridge (2008)	Process	**Strategic**/(Tactical)	Information Security Governance
BSA (2003)	Process	**Strategic**/(Tactical)	Information Security Governance
Clementi &Carvalho (2006)	Process	(Tactical)/**Operational**	ICT Governance
Corporate Governance Task Force (2004)	KPIs	(Strategic)/**Tactical**	Corporate Governance
COSO (2004)	KPIs	Strategic	Organisational governance
Dallas (2003)	KPIs	Strategic	Corporate Governance
Da Veiga, Martins & Eloff (2007)	KPIs	(Operational)/**Tactical**	Information Security
ECUCAUSE (2004)	KPIs	Operational	Information security assessment
Eibl, Von Solms & Schubert (2006)	KPIs	Operational	ICT Management
IP Governance Task Force BASEL II (2007)	KPIs	Tactical	Information Security Governance
ISM3 (2007)	Process	(Strategic)/**Tactical**	Information Security Management
ISO/IEC 27002 (2005)	KPI	Operational	Information security management
IT Governance Institute CobIT T 4.1 (2007)	Process/ KPIs	(Strategic)/**Tactical**	ICT Governance
Kefallinos, Lambrou & Sykas (2009)	Process	(Tactical)/**Operational**	ICT Governance
Kruger & Kearney (2006)	KPIs	Operational	Information security awareness
Ma, Johnson & Pearson (2008)	KPIs	Tactical	Information Security Management
NIST 800-55 (2008)	KPIs	Operational	Information security metrics
NISTIR (2007)	KPIs	Strategic	Information security management
Ostrosky, Leinicke, Digenan & Rexroad (2009)	Process	Strategic	Corporate Governance
Peterson (2004)	Process	Strategic	ICT Governance
Pierce (2004)	Process	Strategic/**Tactical**	Information Management
Poole (2006)	Process	Strategic	Information security management
Posthumus & Von Solms (2004)	KPIs	Strategic	Information Security Governance
Pironti (2007)	KPIs	Operational	Information Security Governance
Weill & Ross (2004) (MIT)	KPIs	Operational	ICT Governance
Westby & Allen (2007)	Process	Strategic/Tactical	ICT and Information security Governance
Williams, TIGS-CMM (2007c)	Process	(Strategic)/**Tactical** /(Operational)	Information Security Governance
Williams, Paul (2001)	Process	Strategic	Information Security Governance
Wolcott Group (2008)	KPIs	Operational	Information Security Governance

ECUCAUSE (2004)

The tool developed by the Security Risk Assessment Working Group of the EDUCAUSE/Internet 2 Computer and Network Security Task Force, is modified from the Corporate Governance Task Force Information Security Governance Framework (2004). EDUCAUSE (2004) developed a scorecard approach to effectively implement information security governance within institutions of higher education such as colleges and universities. The outcome of their research was an extensive list of one hundred security criteria questions organised into five key sections comprising of Organisational reliance on IT, Risk Management, People, Processes and Technology (EDUCAUSE, 2004). Whilst the detailed security evaluation criteria proposed by EDUCAUSE were relevant to this research, the self-reported questionnaire and resultant security rating which ranged from not-implemented to fully-implemented, are reliant on the person completing the

survey's perception of their security behaviours. As such no triangulation was utilised to verify the security measurement outcomes. This approach, whilst relevant to this research, was not considered in its current form to be readily implementable to measure information security governance within General Practice.

EIBL, VON SOLMS & SCHUBERT (2006)

Eibl, von Solms and Schubert (2006) proposed a security rating framework for evaluating the information security of e-learning systems. The framework presents a catalogue of security criteria for which each control is assigned a security strength value, which is summarised into a final single value in order to determine the security rating of the system (Eibl, von Solms and Schubert, 2006). The area of application for the e-learning framework included schools, universities and organisational training (Eibl, von Solms and Schubert, 2006). The final value is computed utilising a mathematical model that is relatively complex for General Practices to implement. Further, the range of security criteria included in the catalogue related to online security issues and was considered incomplete in terms of the range of information security practices required to protect the highly confidential information within a General Practice.

ISO/IEC 27002 (2006)

The International Organization for Standarization (ISO) is "the world's largest developer and publisher of international standards" (ISO, 2009). ISO principles provide 'best practice' guidelines for companies in a wide area of subjects including information security management systems and practices (Calder, & Watkins, 2008). Further, implementation of ISO standards allow organisations to ensure that their "security strategies are co-ordinated, coherent, comprehensive and cost effective" (Calder, & Watkins, 2008). The ISO 27002 (2006) standard, formally the ISO 17799 (2001 & 2005) standard, is an industry benchmark code of practice for information security practice (ISO, 2009). It outlines 11 control mechanisms and 130 security controls (ISO, 2006). The standard establishes guidelines and general principles for "initiating, implementing, maintaining, and improving information security management within an organisation" (ISO, 2006). "The controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment" (ISO, 2006). Further, ISO have defined key information security criteria which can be used to measure security processes. For example, Assessed Security Risks including threats and vulnerabilities can be measured as a percentage of risks identified and assessed as being of high, medium, low or 'unassessed' significance (ISO/IEC 27002). Or cryptographic controls can be measured as a percentage of systems containing valuable/sensitive data for which suitable cryptographic controls have been fully implemented (over a 3 to 12 monthly reporting period) (ISO/IEC 27002). Further, staff training and related security controls are addresses under Human Resources Security inclusive in the security control measures. In this way ISO 27002 provides the KPI measurements required to measure information security processes and procedures within General Practice.

ISO have further defined the ISO 27799-2008 standard for Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799-2008). ISO have recognised the need for "effective IT management in healthcare" due to the increasing use of the Internet and wireless technologies in the delivery of healthcare (ISO 27799-2008). ISO acknowledge that "many healthcare providers operate in small clinics that lack the dedicated IT resources to manage information security" (ISO 27799-2008; IHS, 2008). ISO recommend, regardless of the size of the healthcare organisation, that rigorous controls are put in place to appropriately protect health information (ISO 27799-2008). Further, the ISO 27799 standard identifies the importance of governance as a way to manage information security. To date no Australian organisation including the RACGP and the GPCG have published a full set of guidelines based on this standard.

A further ISO standard, ISO 27004, is under development and will address information security management measurement and metrics. However, whilst this code of practice has not yet been published (ISO, 2009), it confirms the importance of measuring security criteria to measure how well an organisation manages security. Identification by ISO of this standard confirms the necessity for this research.

KRUGER & KEARNEY (2006)

Kruger and Kearney (2006) developed a prototype for assessing information security awareness to promote staff security awareness within organisations. Increased security awareness of employees significantly contributes towards the overall security protection of the organisation (Kruger and Kearney, 2006). The research conducted by Kruger and Kearney (2006) studied and measured the overall effects of staff awareness on security within an international mining organisation. Employees were asked to complete a self-reported, True or False questionnaires. In the collection of such self-reported data, respondents' answers are often in terms of what they believe they do, as opposed to what they may actually do. In this way, the questionnaire may not yield accurate security behaviours. The research conducted by Kruger and Kearney (2006) is informative in its area of application, and staff awareness and security training is considered to be an important aspects of the proposed information security governance framework.

NIST 800-53 (2007)
National Institute of Standards and Technology (NIST) is an American federal agency, the Department of Commerce, who aim to advance "measurement science, standards, and technology" (NIST, 2009). NIST's Computer Security Resource Center has developed a large body of publicity available information and standards with the aim of protecting sensitive data by providing a minimum level of security assurance (NIST, 2009a). NIST (2008) summarises the benefits of using information security measurements to "increase accountability, improve information security effectiveness, demonstrate compliance and provide quantifiable inputs for resource allocation decisions". To achieve this NIST (2008) recommend that a minimum of approximately 140 security baseline controls (security safeguards or countermeasures) are implemented for organisations with 'high-impact' information systems. General Practices fall into this category as their information systems in which "all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a potential impact value of 'high'" (NIST, 2008). This research conducted by NIST will be taken into consideration when developing the proposed information security governance framework.

PIRONTI (2007)
Pironti (2007) investigates effective information security governance as an essential element of corporate governance. He proposes benchmark organisational and performance metrics based on Key Performance Indicators (KPIs). Further, Pironti's (2007) Baseline Metrics Framework, incorporating People, Process, Procedures, Technology and Compliance, promotes meaningful reporting of the metrics framework. Further, Pironti (2007) maps the organisational metrics onto industry benchmarks to determine differences in capability and performance for the organisation. Pironits' (2007) research in regards to motivating the use and implementation of security metrics to measure information security governance is important to this research as it confirms the need for the proposed information security governance framework within General Practices.

WEILL& ROSS (2004)
Weill and Ross (2004) measured ICT governance performance within large organisations by administering a self-reported survey to a minimum of 10 senior managers. Management are required to rate governance outcome and success measure criteria such as cost-effective use of IT, on a continuum from not important to very important (Weill and Ross, 2004). The survey assesses and calculates the importance of a particular outcome to management and how well IT governance contributed to meeting that outcome (Weill and Ross, 2004). The weighted scores outcome mathematically calculates governance performance (Weill and Ross, 2004). This calculation of governance performance offered in research is applicable to the development of the proposed framework although its area of application is broader in that it focused on measuring all aspects of ICT governance.

WOLCOTT GROUP (2008)
The Wolcott Group (2008) assessed information security governance maturity benchmarks based on the ISO 27001/27002 guidelines. The study aimed to measure the effectiveness of organisations to govern information security (Wolcott Group, 2008). The Wolcott Group (2008) emphasise the increasing importance of security frameworks due to legal compliance, internal policy, contractual obligations and public expectations. Implementation of a governance framework has been found to be an "effective, efficient and holistic way to manage information security and to ensure compliance" (Wolcott Group, 2008). The research detailed findings of a large scale research project which analysed security within organisations. The findings detailed the lack of an industry standards based approach by organisations when implementing security management (Wolcott Group, 2008). The research conducted by the Wolcott Group (2008) is relevant to the development of the proposed framework as it recommends that organisations adopt the ISO 27001/27002 framework at a strategic level to "improve security, save resources and to contribute to the success of the organisation" (Wolcott Group, 2008). However, implementation of the ISO 27001/27002 standards in their direct form may not be practical within General Practices as the codes of practice are complex and detailed.

Summary of approaches
The approaches identified in the synthesised table and those discussed in this paper identify hundreds of security controls considered to be important to protect highly sensitive information such as the financial and patient information held by General Practices. As the majority of General Practices are small businesses it is not reasonable to propose that they implement a complex framework designed for large well resources organisations.

Examination of the eight applicable approaches that were synthesised in Table 1, indicate that whilst each approach offers suggestions on managing security, none of the approaches in their current forms are considered to be suitable as a measurement tools, to be directly implemented within General Practice. Further, this research is interested in triangulation of data and therefore developing a governance framework which measures and observes actual security criteria together with perception data as utilised in many of the research approaches discussed in this paper.

Further examination of available security guidelines, most notably developed by the General Practice Computing Group (GPCG), Standards Australia E-Health, ISO 27799, NIST 800-55 and Williams' (2007b) TIGS-CMM governance model, is required. The application of ideas proposed by the other approaches analysed in this paper will also be taken into account when developing a practical information security measurement framework to promote improvement in information security practice within General Practice.

CONCLUSION

Information security is becoming increasingly important in the healthcare sector as legal and accreditation compliance is enforced. Further, General Practices are vulnerable to the same range of security threats and vulnerabilities as are large organisations, but they do not have the same level of available financial and human resources to address information security in the same manner. An extensive review of the literature was conducted to identify applicable approaches for measuring information security governance for use within General Practice. The findings summarised in this paper ranged from single academic research papers proposing a wide range of assessment techniques and tools for security management and governance, to key global organisations such as ISO, NIST and CobiT, who have published extensively in the area of information security and whose measurement techniques have become best practice industry standards. Further, ISO have identified the ISO/IEC 27004 Information security management - Measurement standard to address information security management measurement and metrics (ISO, 2009). This code of practice whilst identified has not yet been publication. Identification by ISO for the need to develop specific standards for healthcare indicates the importance of information security research in healthcare. This further emphasises the importance of this research in developing an Information security governance measurement framework for use within General Practice. The proposed framework will aim to guide decision making and help General Practices to prioritise security activities in order to accomplish a secure computing environment.

REFERENCES

Australian Health Ministers' Conference (AHMC). (2008*). National e-health strategy summary*. Retrieved August 10, 2009, from http://www.ahmac.gov.au/site/home .aspx

Beveridge, C. (2008). *Information governance. Measures for preserving stakeholder confidence*. Retrieved February 22, 2009, from http://www.colin-beveridge.com/index.php/downloads

da Veiga, A., & Martins, N., & Eloff, J. H. P. (2007). *Information security culture – validation of an assessment instrument. Southern African Business Review*, 11(1), 147-166. Retrieved February 20, 2009, from https://www.up.ac.za/dspace/bitstream/2263/5254/1/DaVeiga_Information(2007).pdf

de Haes, S., & Van Grembergen, W. (2004). *IT governance and its mechanisms*. Information Systems Control Journal, 1. Retrieved February 22, 2009, from http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16700&TEMPLATE=/ContentManagement/ ContentDisplay.cfm

EDUCAUSE. (n.d.). *Information security governance assessment tool for higher education*. Retrieved June 22, 2009, from http://net.educause.edu/ir/library/pdf/SEC0421.pdf

Eibl, C. J., von Solms, B. S. H., & Schubert, S. (2006). *A framework for evaluating the information security of e-learning systems*. Retrieved February 28, 2009, from http://www.die.informatik.uni-siegen.de/e-publikationen/Publikationen/2006/ISSEP2006.pdf

Guldentops, E. (2004). *Governing information technology through CobiT*. In Van Grembergen, W. Ed. (2004).Strategies for information technology governance. Idea Group Publishing: Hershey, PA, USA.

Hinson, G. (2006). *7 Myths About Security Metrics*. ISSA Journal, July. Discusses design considerations for a security metrics system, with a few examples.

Kabay, M. E. (2009a). *Security metrics research*. Network World, 27/05/2009. Retrieved June 10, 2009 from http://networkworld.com/newsletters/sec/2009/052509s2.html

Kruger, H. A., & Kearney, W. D. (2006). *A prototype for assessing information security awareness. Computers and Security*, 25, 289-29. Retrieved February 22, 2009, from Science Direct.

Kyereboah-Coleman, A., & Amidu, M. (2008). *The Link Between Small Business Governance and Performance: The Case of the Ghanaian SME Sector*
Journal of African Business 9(1), 121. Retrieved June 17, 2009 from ProQuest Databse.

ISM3 Consortium. (2007a). Information security management maturity model. Compared to ISO27001. Version 2.22. Retrieved June 13, 2009 from http://www.ism3.com/index.php?option=com_docman&task=cat_view&gid=1&Itemid=9

ISO/IEC 17799-2005. (2005). Information technology -- Security techniques -- Code of practice for information security management. Retrieved May 15, 2009 from http://www.iso.org/iso/iso_catalogue/catalogue_ics.htm

ISO/IEC 27002-2006. (2006). International standard - Information technology - Security techniques - Code of practice for information security management. Retrieved May 15, 2009 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103uis.georgetown.edu/departments/eets/dw/GLOSSARY0816.htm

ISO 27799-2008. (2008). Health informatics — Information security management in health using ISO/IEC 27002. Retrieved June 15, 2009 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41298

IT Governance Institute. (2007). CobiT 4.1 Excerpt. Retrieved March 20, 2009, from http://www.itgi.org/Template_ITGI.cfm?Section=Recent_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=45948

National Institute of Science and Technology (NIST). (2009).

NIST. (2009). General information. Retrieved June 2, 2009, from http://www.nist.gov/public_affairs/general2.htm

Nnolim, A. L. (2008). Developing an information security management process model with supporting methodology. Proceedings of the 7th Annual ISOnEworld Conference, June 2-4, 2008, Las Vegas, NV. Retrieved February 22, 2009, from http://www.isoneworld.org

Pironti, J. P. (2007). Developing metrics for effective information security governance. Information Systems Control Journal, 2, 1-5. Retrieved June 22, 2009, from http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=50624&TEMPLATE=/ContentManagement/ContentDisplay.cfm

RACGP (Royal Australian College of General Practitioners). (2005). Security Guidelines for General Practitioners (February 2005). Retrieved June 29, 2009, from http://www.gpcg.org.au/index.php?option=com_content&task=view&id=128&Itemid=38

Rezaee, Z. (2009). Corporate governance and ethics. USA: John Wiley & Sons, Inc.

Uhlaner, L., & Wright, M. (2007). Private Firms and Corporate Governance: An Integrated Economic and Management Perspective. Small Business Economics, 29(3), 225-241. Retrieved June 23, 2009, from ABI/INFORM Global database. (Document ID: 1325026441).

Weill, P., & Ross, J. W. (2004). IT governance : how top performers manage IT decision rights for superior results. Boston, Mass : Harvard Business School Press.

Williams, P. A. H. (2007a). Information governance: A model for security in medical practice. Journals of Digital Forensics, Security and Law, 2(1), 57-72.

Williams, P. A. H. (2007b). An investigation into information security in general medical practice. PhD. Edith Cowan University, Faculty of Computing, Health and Science, School of Computer and Information Science. Perth, Western Australia.

Williams, P. A. H. (2008a). In a 'trusting' environment, everyone is responsible for information security. Science Direct.

Williams, P. A. H. (2008b). The application of CMM to practical medical security capability. Journal: Information Management & Computer Security. 16(1),58 – 73. DOI: 10.1108/09685220810862751. Retrieved June 22, 2009, from Emerald Database.

Wolcott Group. (2008). The 2007 ISO 27001 Benchmark study on information security governance. A benchmark study measuring the effectiveness of organisations to govern information security. Retrieved January 12, 2009 from http://benchmark.wolcottgroup.com

World Bank. (2002). Assessing governance: Diagnostic tools and applied methods for capacity building and action learning. Retrieved January 21, 2009 from http://www.worldbanl.org/wbi/governance

Xenos, (2004). Technical issues related to IT governance tactics: Product metrics, measurements and process control. In Van Grembergen, W. Ed. (2004).Strategies for information technology governance. Idea Group Publishing: Hershey, PA, USA.

COPYRIGHT

Rachel J Mahncke, Donald C McDermid & Patricia A H Williams ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors