2011

Australian primary care health check: who is accountable for information security?

Rachel J. Mahncke
Edith Cowan University

Patricia A H Williams
Edith Cowan University

DOI: 10.4225/75/57b5457ccd8c4
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

AUSTRALIAN PRIMARY CARE HEALTH CHECK: WHO IS ACCOUNTABLE FOR INFORMATION SECURITY?

Rachel J. Mahncke[1] and Patricia A H Williams[2]
[1]School of Computer and Security Science, Edith Cowan University
[2]secau Security Research Centre, Edith Cowan University
[1]r.mahncke@ecu.edu.au, [2]trish.williams@ecu.edu.au

Abstract

Primary healthcare in Australia is vulnerable to a multitude of information security threats and insecure practices. This situation is increasingly important in the developing e-health environment. Information security is everyone's responsibility and it is extensively documented in international standards and best practice frameworks, that this responsibility should be part of formal job descriptions. This necessitates incorporation of security at a functional level for all staff. These responsibilities are integral to demonstrable accountability, together with an authority to take action. Indeed, whilst senior management will ultimately be held accountable, staff need to be aware of the potential issues, given the responsibility to be vigilant, and the authority to act when information security issues arise. This is pertinent within Australian primary healthcare where the accountability for information security is most often devolved to the role of the practice manager. This paper analyses information security accountability from an operational and strategic security capability viewpoint in terms of responsibility and authority. Further, it discusses this in regard to the associated information security governance perspective. In the trustful primary healthcare environment, the accountability for information security resides with operational level staff who have many competing aspects to their role. The paper suggests how to manage this layer of security without burdening the already busy practice manager.

Keywords
Information security governance; healthcare security; governance capability; accountability; general medical practice; CMM.

INTRODUCTION

General practices are usually the first point of contact for people requiring health related care (RACGP, 2005). General practitioners may refer patients onto specialists or hospitals for further expert medical treatment when required. Further, hospitals discharge patients into the long-term care of their general practitioner. As such, general practices are involved in a high percentage of the information exchanges that occur to support the continuation of patient care (NEHTA, 2006).

Information security threats have evolved with 90% of threats now targeting confidential information (Symantec, 2009). The primary motivation of cybercriminals is financial gain either by accessing electronic financial information from a computer system or by stealing personal electronic information with the intent of committing identity theft (Symantec, 2009). Internet enabled general medical practices are vulnerable to the same range of security threats and vulnerabilities as are large organisations, but they often lack the equivalent financial and human resources to address information security in the same manner. Access to information when it is needed at the point of care is vital in healthcare, as it has the potential to impact on human health and lives. Incorporating information security governance into general practice could 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). However, within healthcare, ICT governance does not form part of clinical governance, the healthcare equivalent of corporate governance. Clinical governance includes clinical audit, education and training, research and development, risk management, openness and clinical effectiveness (Starey, 2001). Therefore, implementation of governance activities such as accountability, are not new to general practice.

The Information Security Governance (ISG) capability framework presented in this paper extends available technical best practice information security management (ISM) audits by focusing on the human activities applicable to information security and compliance within general medical practice. An important distinction

needs to be drawn between information security management best practice frameworks such as ISO\IEC 27002 and information security governance. This paper addresses governance capability and accountability for information security within general medical practice. Further, the work presented is an application of the capability maturity model (CMM) technique for information security governance.

GOVERNANCE CAPABILITY

Capability is "the measure of the ability of an entity (department, organisation, person, system) to achieve its objectives" (Business Dictionary, 2011). Governance capability is defined as the measure of ability of practice staff to implement information security governance within the practice in order to meet the practice objectives. Where operational capability is largely technical in nature and therefore the responsibility of the ICT officer/contractor, governance capability is a human endeavour and is the responsibility of designated staff.

To determine governance capability within general medical practice, an information security governance capability framework was developed from the literature (ISO, 2005; CobiT, 2007; NIST, 2003; COSO, 2005). Table 1 lists the eleven areas of information security governance capability that form the general structure of this framework, and maps these to the governance objectives of Accountability, Resource Management and Future Orientation. Further, the table assigns staff roles within a primary healthcare practice that are associated with this responsibility, authority and accountability.

Information Security Governance Capability Framework	**Responsibility**	**Authority**	**Accountability**
Accountability – Aligning information security activities in support of general practice objectives			
1. Strategic Alignment	Practice Manager	Practice Owner	Practice Owner
2. Roles and Responsibilities	All Staff	Practice Manager	Practice Owner
3. Policies	All Staff	Practice Manager	Practice Owner
4. Compliance	All Staff	Practice Manager	Practice Owner
2. Resource Management– Optimising investments in support of the practice objectives			
5. Asset Management	Practice Manager	Practice Manager	Practice Owner
6. Information Management	All Staff	Practice Manager	Practice Owner
7. People Management	Practice Manager	Practice Manager	Practice Owner
8. Financial Management	Practice Manager	Practice Manager	Practice Owner
3. Future Orientation– Appropriate measures to manage risks and potential impacts to an acceptable level			
9. Risk Management	Practice Manager	Practice Manager	Practice Owner
10. Incident Reporting	All Staff	Practice Manager	Practice Owner
11. Business Continuity Management	Practice Manager	Practice Manager	Practice Owner

Table 16: Mapping responsibility, authority and accountability to the Information Security Governance Capability Framework

This governance capability framework has, in addition to the eleven functional areas, sixty associated governance capability measures (not shown). The mapping in Table 1 was developed by taking each category of the governance capability process – accountability, resource management, future orientation – and for each of the eleven functional areas assigning the person(s) with the relevant responsibility for the function, authority to undertake and effect the function, and the person(s) with the accountability for the function. This table highlights the importance of all staff having a role to play in the information security governance process, and not just those with ultimate accountability as is generally thought. Accountability for information security governance, such as legal or regulatory compliance, ultimately rests with the practice owners, however, the Practice Manger is largely left to implement and manage the security tasks as is indicated in the table in the responsibility and authority columns. An understanding of governance roles as they relate to specific aspects of governance capabilities is therefore required.

Accountability

Accountability for information security must be shared by all employees (von Solms & von Solms, 2004; Brotby, 2009). The IT Governance Institute (ITGI) has incorporated eleven control objectives of information security governance in their CobiT benchmarking model (ICT Governance, 2007). As such, information security governance is not seen by CobiT as a separate process to ICT governance, and all information processes are strategically aligned with the businesses' goals and objectives (Poole, 2006; ISO/IEC 27002, 2005). Accountability is also part of both clinical and corporate governance systems (Starey, 2001) and proper information security governance structure is essential **(**von Solms & von Solms, 2004).

The diversity of competing factors in the healthcare environment indicates that information security in practice is a complex issue. It is known that a culture of trust is inherent in healthcare environments and this directly affects policy formulation, creates confidence in staff to maintain confidentiality and privacy, and to implement security measures correctly without scrutiny (Williams, 2008b, 2009). Studies have found that trust in the healthcare environment is driven by group values as well as the trust motivation between individuals thus the creation of a strong trust culture (Zakaria, Stanton & Stam, 2003). In this regard, staff within general practice trust that information security has been adequately addressed by appropriate staff, yet it is not sufficiently communicated or measured across all staff functions.

The framework demonstrates how governance responsibility and authority for information security can be designated to practice staff thereby assisting the practice manager in managing information security. By having an information security governance strategy and training staff to be aware of information security threats to the practice, staff can be given the authority to act in mitigating threats. If this takes place, or is already in existence, then incorporating assessment of the capability of the practice to implement this is required.

MEASURING GOVERNANCE CAPABILITY

Developed in the late 1980s, Capability Maturity Model (CMM) was devised to drive and guide improvement through the appraisal of internal and external organisational processes (Galin and Avrahami, 2006). Thus, CMM provides a logical progression from ad hoc process implementation to regimented and definite process execution. In this manner it is possible to use CMM to assess and measure process areas for identification of weaknesses in organisational operations and practices (Hopkinson, 2001). Further, the CMM approach has been demonstrated to be an integral part of CobiT, an ICT governance framework. (Brothby, 2009, pg 10). The success factors in the use of CMM have been shown to be positively related to planning and tracking of activities. Amongst the suite of CMM derivatives are those relating to medical practice security.

Research conducted by Williams (2008a) demonstrated the feasibility of using a Capability Maturity Model (CMM) approach to benchmarking levels of operational information security within general medical practice. "When implementing the operational [CMM] framework, each process for a given activity can be addressed individually for contribution to a level above. This means that improvements can be incremental and competency can be tracked using the specified criteria" (Williams, 2008a). It is therefore proposed that CMM is likewise a suitable approach to measure information security governance capability.

As defined by Williams (2008a) the CMM assessment levels that are applicable to the medical environment for practical application are defined in Table 2. These levels are the basis for the CMM levels as defined in the application in Table 3.

CMM Level	*Operational Focus*
5 Optimizing	Best practices are followed and automated
4 Managed	Processes are monitored and measured
3 Defined	Processes are documented and communicated
2 Repeatable	Processes follow a regular pattern
1 Initial	Processes are ad hoc and disorganised.

Table 2: General characteristics of CMM (Williams, 2008a)

Whilst CMM can be somewhat "imprecise and subjective, it does however, provide a straightforward intuitive approach that most staff would find sufficiently easy to apply" (Brothby, 2009, pg 10). The benefit of the CMM approach therefore is that general practice staff without ICT training are likely to find the approach to measuring governance easily understandable.

Table 3 below develops an example using one of the eleven information security governance framework areas outlined in Table 1. It has been informed by the Australian Flexible Learning Framework's (2001) BECTRA matrix. The BECTRA matrix is an e-learning strategy that assists organisations to determine a baseline in order that they may improve their practice. The matrix is itself an adaptation of a performance improvement (PI) research tool developed by organisational change (International Society for Performance Improvement, 2011). Table 3 below is an adaptation of one section of this matrix, *Vision and strategic planning.* The approach of the BECTRA matrix is unique in that staff without specific governance knowledge are easily able to map their organisations performance to the criteria presented within the matrix. For this reason, the user friendly BECTRA governance approach has been utilised for this governance capability framework.

The framework is utilised as follows: for each aspect in the matrix, a practice selects the appropriate information security governance (ISG) functions applicable to the practice from the range, Initial through to Optimised. An ISG baseline is established after the first iteration of the matrix is complete. The framework is flexible in that a practice can customise it to suit their needs. The practice should aim for incremental improvement from the baseline until the 'Managed' metric, or above, for each ISG function in the matrix has been achieved.

1. Strategic Alignment				
1.1 Development of an information security governance (ISG) strategy within the general practice				
Initial	Repeatable	Defined	Managed	Optimised
Work has not begun on developing an ISG strategy within the practice.	The ISG strategy is still in draft form.	An ISG strategy has been published but it is not yet a key driver for change within the practice.	Staff across the practice actively contribute to the process of implementing, updating and developing the ISG strategy.	Aspects of the ISG strategy are cross-referenced to other strategy and policy documents and is a key driver for change across the practice.
1.2 Communicating the ISG strategy across the practice				
Initial	Repeatable	Defined	Managed	Optimised
No communication of the ISG strategy to staff or patients has taken place.	Staff and patients are largely unaware of any practice strategy for the development of ISG.	Communicating the strategy to staff and patients has started, but as yet awareness of the strategy is limited to a minority of staff.	Senior staff have taken appropriate opportunities to communicate the strategy and as a result most staff and some patients are aware of it.	All staff and the majority of patients are aware of the practice's ISG strategy.

1.3 Relationship of ISG strategy to other strategic plans				
Initial	Repeatable	Defined	Managed	Optimised
There is no reference to ISG in the practice's other strategic plans.	There are a few mentions of ISG in the practice's other strategic plans.	There is some cross-referencing between the ISG strategy and other strategic plans.	There is comprehensive and clear cross-referencing between the ISG strategy and the practice's other strategic plans.	The vision for the development of ISG is embedded in all strategy documents, and clearly contributes to the practice's overall vision and goals.
1.4 Strategic approach to the management of ISG				
Initial	Repeatable	Defined	Managed	Optimised
There is no strategic management of the ISG strategy.	Management of ISG takes place only within one team or section of the practice.	There are some links between different sections of the practice in terms of the management of ISG.	There is a strategic approach to the management of ISG across the whole practice.	The management of ISG takes place within a strategic framework. There is strong leadership from management and appropriate delegation of operational IS decision making.
1.6 Monitoring and reviewing the ISG implementation				
Initial	Repeatable	Defined	Managed	Optimised
No monitoring or reviewing activity has taken place.	Implementation of the ISG strategy has only rarely been monitored, reviewed or evaluated in any detail.	Some aspects of the ISG strategy are monitored and reviewed, but this is not done in a systematic way, makes no reference to other practice strategies, and does not involve all stakeholders.	The ISG strategy is regularly monitored, reviewed and evaluated in the context of the practice's other policies, and in line with the practice's goals and involves all stakeholders.	The practice has a well established ISG framework for monitoring and reviewing all its strategies and policies.

Table 3: Strategic Alignment CMM

Once the practice has established a baseline, improvements in information security governance practice can be achieved in an ongoing and sustainable manner by addressing and actioning each area where improvements are needed. Further, general practices can perform a gap analysis to determine their information security governance goals in relation to the practices overall objectives. Once the expectation of information security performance in the practice is understood, it is possible to compare that expectation with the practices current level of information security performance. This comparison becomes the gap analysis.

CONCLUSION

Governance capability is linked to accountability in that staff need to be aware of, and possess the skills needed, to implement information security governance. Further, to be accountable for information security, general practices need to comply both with legal and best practice standards. In order to establish information security governance within the general practice, available resources must be known and constraints understood.

Empowering staff with the supporting mechanisms to properly perform their information security responsibilities thus forms the basis of their governance capability.

The information security governance capability framework presented in this paper is the basis of ongoing doctoral research. The purpose and objective of the framework is to promote improvement in information security practice given the current threat environment. Further, the flexibility of the framework will assist practices in developing an information security strategy. The framework enables the practice to establish a baseline and raise staff awareness of information security requirements within the practice. It also creates a conduit for distributing responsibility and authority for information security to designated practice staff thereby assisting the practice manager in managing the information security function. By having an information security governance strategy and training staff to be aware of information assets and the need to be protected within the practice, staff can be given the authority to act.

The aim of the framework is to assist practices without overly burdening them with additional work flows. Information security governance is a sizeable task for practices to integrate into their normal, and arguably more important, patient and management tasks. The framework contributes towards better security practice within the practice, and contributes towards cyber resilience and the protection of sensitive information. It will assist practice owners to meet their responsibilities for information security governance and ensure a well protected practice. Ultimately, it is the general practices' themselves and the professions that will need to prioritise and drive these initiatives.

REFERENCES

Australian Flexible Learning Framework. (2008). Tour 5: Prepare an e-learning plan: BECTRA matrix. Retrieved October 31, 2011 from http://designing.flexiblelearning.net.au/tours/tour5_develop_plan.htm

Business Dictionary. (2011). Capability. Retrieved October 31, 2011 from http://www.businessdictionary.com/definition/capability.html

Brotby, K. (2009). *Information Security Governance. A Practical Development and Implementation Approach*. New Jersey: John Wiley & Sons, Inc.

COSO. (2005). Putting COSO theory into practice. Retrieved June 2, 2009, from http://www.coso.org/resources.htm

Galin, D. & Avrahami, M. (2006). Are CMM program investments beneficial? Analyzing past Studies. *IEEE Software*, *23*(6), 81-7.

Hopkinson, J.P. (2001). *The relationship between the SSE-CMM and IT security guidance Documentation.* Retrieved from http://www.sse-cmm.org/docs/sse-guides.pdf

International Society for Performance Improvement. (2011). International society for performance improvement. Retrieved October 31, 2011 from http://www.ispi.org

International Standards Organisation. (2005). ISO/IEC 27002-2005: 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.html

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

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.

National Institute of Science and Technology (NIST). (2003). Security Metrics Guide for Information Technology Systems. Special Publication 800-55.

NEHTA. (2006a). Towards a Secure Messaging Environment. An E-Health Transition Strategy. Version 2.0 Final.Retrieved November 8, 2006 from http://www.nehta.gov.au/component/option,com_docman/task,cat_view/gid,129/Itemid,139/

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

Poole, V. (2006). Why information security governance is critical to wider corporate governance demands – a European perspective. Retrieved February 22, 2009, http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=30681&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

Starey, N. (2001). 'What is clinical governance?'. Evidence-based medicine, Hayward Medical Communications. Retrieved October 31, 2011 from http://www.medicine.ox.ac.uk/bandolier/painres/download/whatis/WhatisClinGov.pdf

Symantec. (2009). Symantec Internet Security Threat Report Finds Malicious Activity Continues to Grow at a Record Pace. Retrieved October 21, 2010 from http://www.symantec.com/about/news/release/article.jsp?prid=20090413_01

von Solms, B., & von Solms, R. (2004). *Computers & Security 23*(5),37 Retrieved October 17, 2011 from http://www.tut.fi/units/tuta/tita/2006-2007/TITA-5300/10sins.pdf

Williams, P. A. H. (2008a). 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.

Williams, P.A.H. (2008b). In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report, 13(4), 207-215.

Williams, P. A. H. (2009). What does security culture look like for small organizations? In C. Bolan (Ed.) *Proceedings of the 7th Australian Information Security Management Conference*, (pp.48-54), SECAU Security Research Centre, Edith Cowan University, Perth, WA.

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).

Zakaria, N., Stanton, J. & Stam, K. (2003). Exploring security and privacy issues in hospital information system: An information boundary theory perspective. *AMIA 2003 Symposium Proceedings* 1059.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the prior discourse and publications together with Associate Professor Donald McDermid in the area of information security governance within general medical practice.