2010

An Information Security Governance Framework for Australian Primary Care Health Providers

Donald C. McDermid
Edith Cowan University

Rachel J. Mahncke
Edith Cowan University

Patricia A H Williams
Edith Cowan University

DOI: 10.4225/75/57b6734334780
Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

An Information Security Governance Framework for Australian Primary Care Health Providers

Donald C McDermid[1], Rachel J Mahncke[1], Patricia A H Williams[1,2]
[1]School of Computer and Security Science
[2]secau - Security Research Centre
Edith Cowan University
Perth, Western Australia
d.mcdermid@ecu.edu.au

Abstract
The competitive nature of business and society means that the protection of information, and governance of the information security function, is increasingly important. This paper introduces the notion of a governance framework for information security for health providers. It refines the idea of an IT Balanced Scorecard into a scorecard process for use in governing information security for primary care health providers, where IT and security skills may be limited. The approach amends and justifies the four main elements of the scorecard process. The existence of a governance framework specifically tailored for the needs of primary care practice is a critical success factor if such organisations are to move to a robust level of information security. The challenge is twofold. Firstly, measures for governance need to be understandable to the target audience using the framework. Secondly, the number of measures needs to be controllable otherwise the process will become unviable and unused. This research synthesizes existing models and industry standards to formulate a new governance process that meets these two important criteria. The contribution of this research is in the refinement of governance metrics to make them useful to healthcare providers, specifically in relation to IT and new information communication technologies.

Keywords
Governance, information security, general practice, framework, health

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 medical practices, as the primary point of care, is critical to the success of an interoperable healthcare system. Protecting patient health information requires appropriate security measures with regard to technologies, policies, and processes as well as ensuring that staff are trained and aware of security activities. But achieving industry security standards is problematic since arguably current standards are not designed for small organisations such as a general practices. Yet, nothing less than full industry standard security is acceptable if practices are to meet the rising number of computer security threats and provide a secure environment for patient data. General practices need a framework of accountability and control to address and demonstrate effective information security governance.

A small business is defined by the Australian Bureau of Statistics (2001) as a "business employing less than twenty people". According to the Australian Bureau of Statistics (2001) there were 9,600 general practice businesses employing 56,911 persons of which 20,825 (38 per cent) were medical practitioners. Small medical practices with one to two medical practitioners accounted for the "majority (55 per cent) of employment in the industry" (Australian Bureau of Statistics, 2003). This means that the majority of general practices are small businesses.

This is highly significant because small general practices behave quite differently to large organisations. For example, they lack financial resources and time. This in turn manifests itself in many ways. For example it breeds of culture of cost accountability for every financial outlay made. Lack of time and knowledge also stops them from accessing and tailoring research on information security in larger organisations to fit their small business needs. Further, general practices are unlikely to employ dedicated Information Communication and Technology (ICT) staff within the practice. Thus keeping up-to-date with information security practices is an added burden on practices that are already overly busy and short staffed.

Whilst some information security practices within general practice are similar to that required in other small businesses, there are added legal and accreditation responsibilities, compliance requirements and far greater impacts and repercussions should patient information be misused. A critical factor is that general practices do not have the dedicated number of employees or multiple levels of management that exist in large 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 so still need to meet a minimum standard to protect their information. All general practices still need to address accreditation and compliance criteria.

So, a major challenge for all small businesses and in particular general practices is to distill from the plethora of standards designed for large organisations (for example ISO 27799-2008 2008; NIST 2009; ITGI 2007), a set of standards and guidelines that are both relevant and practical. This raises questions of who would have the skill and knowledge to undertake this, 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. Clearly the introduction of an information security governance framework tailored specifically for medical general practice that improves compliance, monitoring and measurement of information security practices would be a step forward.

Currently the best source of security guidelines available for general practitioners in Australia is provided by the Royal Australian College of General Practitioners (RACGP) through the General Practitioners Computing Group (GPCG). Specifically these are the GPCG's Security Checklist and Security Template for Computer Security Policies and Procedures Manual (GPCG 2004a; 2004b). Made available to general practitioners in 2005 they were a significant step forward for general practices compared to what was previously available. However, their uptake has been limited. One reason for this is that there is arguably insufficient support for implementing these guidelines – specifically there is no governance framework to support this change process.

In summary the situation in Australia can be characterized as unclear and unhelpful for general practices. On the one hand they are treated as relatively independent small businesses expected to resource security solutions by themselves and at their own cost. On the other, they are legally required to comply with the law and meet the expectations of government and patients in respect of information confidentiality. From a pragmatic perspective, without an appropriate governance framework that is sufficiently tailored to the needs of Australian general practice, it is unlikely that much progress will be made by general practices on their own.

In this paper we present an overview of an information security governance framework with particular focus on the elements of how information security should be governed in a general practice. We introduce the concept and need for a governance framework. The concept is based on the seminal work of Kaplan and Norton (1992) and later Van Grembergen (2000). This is followed by sections outlining the essential elements of governance. By elements we mean those major areas or groupings of governance activity that facilitate due diligence to the principles and practicalities of governance.

AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

Information security governance is usually considered part of IT Governance, which itself is a key asset area of corporate governance (Pironti, 2007). Corporate governance typically comprises three core elements 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). However, it is clear that there is more work to be done in developing a framework that is tailored to the needs of Australian general practices. In essence, such a framework would be a guide to a general practice and a resource enabling a general practice to review its information security practices. It will also define its legal obligations no matter what their current level of compliance is and if necessary, provide guidance to move to a higher level of compliance.

A primary and critical aspect of any governance framework is that much of the challenge lies with the management of, in this case, the general practice. It is how the structures within the practice are set up and maintained, the lines of reporting, decision-making, participation of staff and so on that will largely determine how effective a framework is in bringing about change. Secondly, it needs to be recognized that across Australia, general practices will be at different levels of development in respect of how well they actually manage to provide a secure environment for their data. So any framework needs to be comprehensive enough to deal with different stages of development and further facilitate movement upwards to better levels of security.

McDermid, Mahncke and Williams (2009) provide a definition of information security governance framework for a medical general practice as follows:

An information security governance framework is a set of structured guidelines containing a collection of resources including ***people, processes, policies, measures, controls*** *and* ***training*** *designed to achieve and* ***continuously improve*** *upon industry standard information security in medical general practice.*

In order to provide a deeper appreciation of this definition and its implications for governance, each of the highlighted words in the definition will now be discussed.

People are fundamental to successful governance. Who will be assigned which tasks and responsibilities? Who reports to whom? General practices differ in how they are organised. In some though not all practices much of the administration and decision-making is passed over to practice managers allowing doctors to concentrate on what they are 'good at'. Is this wise? Should doctors abrogate issues of patient confidentiality to others? What kind of shared decision-making is appropriate for such matters?

A set of **processes** needs to be defined and aligned to the responsibility and accountability structure defined by management and again, by its very nature this will vary across practices for a number of obvious reasons.

Policies that specify each area that requires monitoring need to be defined clearly and simply yet pragmatically. Policies are required for areas such as data backup, encryption, disaster recovery, wireless, mobile, intrusion detection to name but a few.
Measures are key to the framework. Measures establish whether the practice is meeting an aspect of information security. For example, a measure might be the number of attempted breaches to the practice computer network in the last month. Measures must be practical and helpful to the practice in terms of identifying risks or matters that need attention. As discussed earlier, the current guidelines of the GPCG do not go far enough in terms of providing measures that meet industry standards and that provide practices with usable and practical feedback on how shortcomings can be improved.

Controls form the backbone of any governance framework. Here controls include defining accountabilities, responsibilities and audits. Much of accountability is defined by law in respect of who are the legal custodians of information in a practice. A practice needs to determine the extent to which what is actually happening in a practice complies with the law. This would be the starting point for defining controls. For example, whilst a doctor may not be expected to perform a daily back up of data, a doctor might be appointed as accountable for ensuring that this was done regularly according to process and also for checking in some appropriate manner that this was being done. An appropriate manner for instance might be that the practice manager actually conducts the check and reports at a monthly meeting to the doctor(s) who is accountable. Responsibilities are those allocated duties and tasks carried out by all stakeholders in the practice from doctors to receptionists. Clearly responsibilities must be aligned to accountabilities and checked regularly. Lastly, audits are one important type of verification process carried out that provides feedback on what is actually happening as opposed to what is supposed to be happening.

For a practice to be current with all compliance, regular training and refresher **training** will form an important component of a practice's activity.

Lastly, the definition of a governance framework is not complete without a statement focusing on **continuous improvement**. In many ways the element of continuous improvement is the most important aspect of a governance framework because the framework should allow for improvement. Thus breaches, weaknesses or failures become opportunities for improvement within a controlled framework.

THE ELEMENTS OF AN INFORMATION SECUIRTY GOVERNANCE FRAMEWORK

A well established landmark in governance literature was the work done by Kaplan and Norton (1992, 1993, 1996a, 1996b) when they introduced the balanced scorecard for the enterprise. The idea behind a balanced scorecard is that the evaluation of an organisation should not be restricted to financial evaluation but could and should be supplemented with metrics concerning internal processes, future aspirations as well as customer satisfaction. Organisations were encouraged to evaluate themselves across a broader range of metrics and in doing so take a more balanced and comprehensive snapshot of their overall performance.

Van Grembergen (2000) developed this idea and made it relevant to the domain of information technology by arguing that the four specific metrics used on a Kaplan and Norton's scorecard for a business may not relate directly to service departments within an organisation such as information technology. Van Grembergen's four metrics were operational excellence, user orientation, future orientation and business contribution. A contribution of this paper is to refine these metrics and apply them to information security governance for general practices, since information security is indeed only one component of information technology. This paper will demonstrate that further refinement of the types of metric (element) is appropriate for information security governance purposes.

Figure 1 shows an information security governance framework with four elements:

- Operational excellence
- Accountability
- Future orientation
- Resource management

Deploying a governance framework would require that at governance review meetings each of the four elements be considered when discussing governance. It would operate in practice as follows. The meeting would review all incidents that had occurred over the period as well as details of security performance. The meeting would be asked to consider whether any incident, operational performance measure or periodic audit justified changes to the detail of the operation excellence, accountability, future orientation or resource management elements. For ease of distinction we suggest the term *measure* is used here when describing aspects of operational performance (e.g. number of breaches per time period) and the term *metric* is reserved for summarizing the performance of a complete element of the governance framework such as operational excellence.

In the following sections each of the elements is discussed in detail and the rationale for their title is justified.

OPERATIONAL EXCELLENCE

Operational excellence refers to how well an entity is performing its basic operational activities. For information security these would be the range of capabilities necessary to ensure the confidentiality, integrity and availability of patient and practice data in a medical general practice. So the term used by Van Grembergen is appropriate here in relation to information security.

The headings for these 'information security capabilities' are human resource security, information assurance, physical security, access control, practice systems, network security, information exchange and monitoring. For instance, an acceptable human resource security capability would require that all staff including third parties were, for example, given access to, trained in, resourced in and most importantly following information security policies before, during and after employment.

At each governance meeting a report would be provided showing operational performance across the range of capabilities together with any incidents that had been reported. Further if periodic audits had been conducted then the results of these would also be discussed. Audits are an important addition to incidents and measures. Audits are physical inspections that policy is being followed as it is possible that discrepancies may not show up as incidents or in the measures taken. All these inputs would drive the discussion. It would be the task of the governance meeting to re-affirm or otherwise the operational excellence metric and if necessary explore any implications for the accountability, future orientation and resource management elements.

ACCOUNTABILITY

The term accountability has been chosen in preference to the term user contribution on the IT Balanced Scorecard (van Grembergen 2000). Clearly IT departments provide a service to the organisation and so it makes sense to gauge from users how well they are perceived to perform that function. Information security on the other hand is more of a control that must be addressed within a general practice than a function per se and of course often users (patients) will not be aware of how well that function is being performed. The term accountability seems to capture this need more aptly. In particular, compliance to legal requirements, the structures used within the practice to govern information security and the quality of the policies being utilized are considered as directly contributing to accountability.

Compliance

It is only correct and natural that general practices see their prime role as helping the patient. Yet they have obligations under numerous acts of parliament to ensure the confidentiality, integrity and accessibility of their patients' data. Thus compliance to legal obligations is seen as the main driver or motivation here. Relevant acts are the Privacy Act (1988), the Privacy Amendment (Private Sector) Act (2000), the National Health Act (1953), the Electronic Transactions Act (1999) and the Freedom of Information Act (1982).

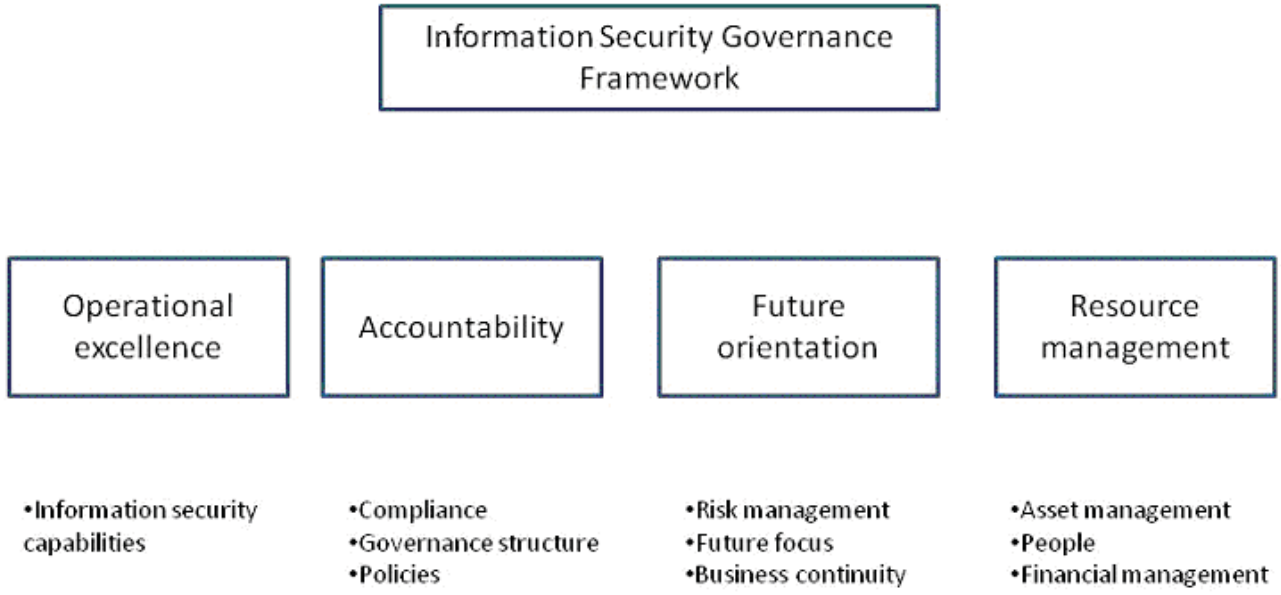

Figure 1. An Information Security Governance Framework

Governance structure

As introduced in an earlier section, how information security governance is defined within the practice is fundamental. The most important aspect of this is that the governance structure must fit the practice. So answering questions such as how many meetings will we have, who should attend, who is responsible for what, what are the lines of authority and responsibility and so on, all have to be workable and seen as working. If not they need to be reviewed and changed. Aspects of incidents or audits may highlight weaknesses in this structure.

Policies

The quality of the information security policies is paramount and again it is likely that incidents, measures or audits will uncover areas for improvement. When such events are highlighted, the emphasis should be on how the policies can be improved to obviate similar problems in the future.

FUTURE ORIENTATION

Whereas accountability to a large degree asks questions about how the practice is currently performing its information security governance, future orientation, as the name implies, suggests that it is also necessary to deal with aspects of current vulnerabilities (arising out of incidents, measures and audits) that have implications in the future. In other words, having dealt with the present (under accountability) we move to future orientation to evaluate the practice in terms of potential future implications and consequences. The three aspects of future orientation we have identified are risk management, future focus and business continuity.

Risk management

Any issue identified for discussion at a governance meeting needs to be considered here as a potential future risk under risk management. An essential purpose of risk management is to assess how detrimental or damaging the consequences of an issue could be so that a decision can be taken to reduce the likelihood of similar occurrences in the future. For example, it may be decided to explore the option of a more expensive hardware firewall in order to stem the rise of attempted breaches to the network that are currently occurring.

Future focus

The purpose of future focus is to enter into a discussion of where the practice is in terms of its aspirations to improve its information security practices. It may be that the practice desires to reach a high level of security in a certain timescale and so a regular item at a governance meeting would be to track progress against that goal.

Business Continuity

Some issues arising may well have implications for disaster recovery and business continuity. For instance what if an audit discovered that the backups for the last three months were useless? Again, the over-riding role of any governance meeting is to ensure that the governance framework and its processes are working rather than necessarily solve specific problems at the meeting itself.

RESOURCE MANAGEMENT

Van Grembergen's fourth title is business contribution on the IT Balanced Scorecard (2000). The idea is that assessing IT's contribution to the business is a good way of putting a cost benefit perspective on the work done by IT. However, given that the main driver for information security in a general practice comes from compliance a more appropriate label for this is arguably resource management. Here resource management is defined to include the main resources that contribute to information security i.e. asset management, people and financial management. Logically, resource management is considered towards the end of a governance discussion since all the factors and risks need to be aired first so that a proper cost – benefit – risk evaluation can be undertaken.

Asset Management

The collection of all hardware and software constitutes the IT assets of a general practice. Constant maintenance and updating is required to ensure the integrity of the systems deployed. Issues arising under any of accountability, operational excellence or future orientation may require renewal or upgrading of assets. Under asset management there should be a plan for renewal and upgrading, contractual and support details, all of which are relevant inputs to a decision concerning assets.

People

Clearly, people are at the heart of successful governance. They will make or break it. So having discussed an issue previously as an 'issue', it may be that there is appropriate cause to reconsider responsibilities, incentives, rewards, training, re-alignment of duties etc under this heading from a governance perspective.

Financial Management

Finally, as most decisions have a financial component and remember there may be many decisions that have to compete within a limited budget, committing funds to address and remove issues is a logical concern towards the end point of a governance meeting.

SCORECARD PROCESS

Having described each of the scorecard elements it now remains to describe the process of assigning a score to each element. Typically this would occur at the end of a governance meeting and would involve reviewing previous element scores. Each element would be reviewed in turn. By reviewing the issues that arose during the meeting an assessment would be made in terms of whether it was felt that the score of the element was static, worse or better and the score changed to reflect that perception.

Once this is done for all four elements, it is important for the meeting to discuss the overall progress that the general practice is making with respect to governance. Is it on track? What areas are deficient and why? What can be done to correct deficiencies? The interplay between the elements is significant as it allows the meeting to reflect on progress with respect to different aspects of the 'small business', that is, operational excellence, accountability, future orientation and resource management. Arguably this is a most valuable exercise that assists the practice in focusing on what is important.

SUMMARY AND FUTURE RESEARCH

This paper introduced the notion of a governance framework for information security for a general practice and provided a definition thereof. It developed the idea of an IT Balanced Scorecard into a scorecard process that could be used to govern information security in a general practice, amending and justifying the elements of the scorecard in the process. The existence of a governance framework specifically tailored to the needs of general practice is seen as a critical success factor if general practices are to move to a robust level of information security.

At the time of writing the detail of the information governance framework is close to completion. The area requiring most effort is in developing measures. Work done by Williams (2008) demonstrated the feasibility of using a Computer Maturity Model approach to benchmarking levels of information security and at the time of writing this has been operationalised across all areas relevant to information security in a general practice. We have almost finalised the definitions of simple useful measures that can best benchmark for example how many intrusions were detected over a time period and how many of these were either denied or breached. There are two challenges here. The first is that these measures need to be understandable to doctors and other practice staff for true governance to occur. After all, they are not typically IT experts. Secondly, there is a real danger that the number of measures required will be such as to make the whole process unviable. So here the task in defining the framework has been in asking what is the minimum set of measures required to achieve the goals of this framework.

In order to test the framework a programme of action research is planned in which the framework will be implemented in a number of general practices across Western Australia. The feedback from this study will provide valuable insight in relation to the two challenges mentioned above in particular whether the measures are sufficient to adequately cover all important aspects of governance. Achieving the right balance is critical to the success of this program.

REFERENCES

AHMC. 2008. The Australian Health Minister's Conference . Retrieved July 14, 2009, from http://www.ahmac.gov.au/cms_documents/National%20E-Health%20Strategy.pdf

Australian Bureau of Statistics. (2001) 1321.0 - Small Business in Australia, 2001. Retrieved May 11, 2009 from http://www.abs.gov.au/AUSSTATS/abs@.nsf/ProductsbyTopic/97452F3932F44031CA256C5B00027F19?OpenDocument

Australian Bureau of Statistics. (2003). Australia's private medical industry 2110-2002.Retrieved June 22, 2009 from http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8685.0Main+Features12001-02?OpenDocument

Electronic Transactions Act. (1999). Retrieved June 2, 2009, from http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256

Freedom of Information Act. (1982). Retrieved June 2, 2009, from http://www.austlii.edu.au

GPCG (General Practice Computing Group). (2004a). Security guidelines for general practitioners. Retrieved June 22, 2009 from http://www.gpcg.org.au/index.php?option=com_content&task=view&id=128&Itemid=38

GPCG (General Practice Computing Group). (2004b). Computer security checklist. Retrieved June 22, 2009 from http://www.gpcg.org.au/images/stories/pdfs/publications/docs/2004Phase1Proj/Securitychecklist.pdf

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

ITGI. (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

Kaplan, R. and Norton, D. (1992). "The balanced scorecard — measures that drive performance," *Harvard Business Review.* January-February, pp. 71-79.

Kaplan, R. and Norton, D. (1993). "Putting the balanced scorecard to work," *Harvard Business Review*. September-October, pp. 134-142.