12-1-2009

Challenges in Improving Information Security Practice in Australian General

Donald C. McDermid
Edith Cowan University

Rachel J. Mahncke
Edith Cowan University

Patricia A. Williams
Edith Cowan University

DOI: 10.4225/75/57984ef031b4c
7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

Challenges in Improving Information Security Practice in Australian General Practice

Donald C McDermid[1], Rachel J Mahncke[1] & Patricia A H Williams[1,2]

[1]School of Computer and Security Science
Edith Cowan University

[2]secau – Security Research Centre

Abstract

The status of information security in Australian medical general practice is discussed together with a review of the challenges facing small practices that often lack the technical knowledge and skill to secure patient information by themselves. It is proposed that an information security governance framework is required to assist practices in identifying weaknesses and gaps and then to plan and implement how to overcome their shortcomings through policies, training and changes to processes and management structure.

Keywords

Governance, information security, general practice

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. Yet the contribution of general medical practice will falter unless information security practice within general medical practice is perceived to be up to an acceptable standard. 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 full blown industry security standards is problematic since it is contended that current standards are not designed for small organizations such as medical general practices. Yet, nothing less than full industry standard security is acceptable if practices are to meet the rising number of computer security threats now occurring 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.

In this paper we review the status of information security in Australian medical general practice and outline the challenges within. In the next section we review where Australian practices are today by discussing the compliance environment, available resources and the national infrastructure that supports general practices. This is followed by outlining where Australia (and indeed any nation) would want to be in relation to sound information security for general practice. Finally, there is a brief discussion on what has to be done to get there.

WHERE ARE WE TODAY?

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 (2003) 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 organizations. For example, they lack the financial resources and time which manifests itself in many ways for example it breeds a 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 organizations to fit their small business needs. Further, general practices are unlikely to employ dedicated Information Communication and Technology (ICT) staff within the practice and so keeping up-to-date on information security practices is an added burden on practices that are already overly busy and short staffed.

Whilst some information security practices within general practices are clearly similar to what is 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 organizations. Large organizations 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 organizations and so still need to meet a minimum standard to protect their information. General practices therefore still need to address accreditation and compliance criteria.

That said a major challenge for small businesses in particular is to distil from the plethora of standards designed for large organizations (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 in a practice 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 to general practices compared to what was previously available. However, whilst most practices are aware of them, there still remain many difficulties with their uptake (Williams, 2007). The following is a suggested list of reasons why this has been so.

Firstly there is the 'checklist gap'. This is a gap between what is specified in the guidelines and what a particular general practice needs to know in order to carry out that guideline. For example, the checklist for data back-up requires that a date when the back-up procedure was last tested is provided. The question arises as to what is a reasonable timescale for re-testing a back-up procedure? One month? Three months? The guidelines themselves do not provide this level of advice or support. To be fair, the guideline makes that point that 'it is very difficult to provide a guideline that will suit all practices' (GPCG, 2004a). That said the real question is to consider the likely reaction of most practices to that lack of specificity. Unless the security coordinator in the practice has a good background in security it will be difficult for a general practice to take the guidelines as they stand and make direct use of them. Thus many such similar problems with the checklist gap serve to reduce uptake of the guidelines, simply because there is not enough direct guidance or advice.

Secondly, in 2004 direct funding of ICT support for general practices was withdrawn by the Government. Previously there was some degree of support offered by Divisions – each Division was responsible for supporting a set of practices within a geographical area across a range of functions including ICT. When the funding was withdrawn the ICT support functions in the Divisions were cut back often to a single person who performed more of a coordinating role to outside services such as GP networks who for a fee for service will provide support and training. Outsourcing ICT in this way has further issues such as giving access of confidential information to external contractors, although contractual agreements with third parties (often overlooked) can remedy this situation (Standards Australia E-Health, 2003). However, adherence to routine security practices such as encrypting an email containing confidential information, remain the responsibility of the general practice despite outsourcing ICT functionality. Given the small business mentality prevalent in general practices the above withdrawal of funding has therefore caused difficulties in uptake of the guidelines.

The third reason is a lack of strong and clear direction from Government for general practices. The Government authority responsible for e-health is the National E-Health Transition Authority (NEHTA). However NEHTA's main focus currently and for some time now has been the implementation of coding standards, Australia's interoperable healthcare system and the Individual Electronic Health Record (IEHR) (NEHTA, 2006). Now whilst these are clearly important and necessary goals, attention to such matters has led to NEHTA not providing leadership to general practices in regard to specific standards, obligations and responsibilities in respect of information security and this has led to uncertainty over the Government's commitment to enforce the numerous acts in this area (for example Electronic Transactions Act 1999; Freedom of Information Act 1982).

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 morally if not legally expected to meet the needs of the law, government and their patients in respect of patient confidentiality.

WHERE DO WE WANT TO BE?

It is clear from the above that there is still much more that needs to be and could be done in terms of facilitating and supporting improvement. What is required is to stimulate the process by making it easier for individual practices to access expertise and implement the necessary change in their practice. It is suggested that this needs two critical stimulants both of which are vital if this is to happen.

The first is a governance framework that can take a general practice, no matter what stage it is at and with support, move it to the next level. The second is their needs to be an appropriate push downwards from government in the form of an accreditation system that mandates that practices enter this program and progress upwards within it.

An information security governance framework

A primary and crucial 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, across Australia general practices will be at different levels of development in relation to 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 security. Thirdly, since no such full governance framework has yet been articulated it is necessary to specify to an appropriate level and conduct confirmatory research into defining an information security governance framework that performs its stated role.

As a working definition, the following is submitted: *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.*

Each of the key words in the definition will now be discussed in order to provide the reader with a sense of what is envisioned. Clearly people are fundamental. Who will be assigned which tasks and responsibilities? Who reports to whom? General practices differ in how they are organized. In some though clearly 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 whole array of processes need 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 data backup, encryption, disaster recovery, wireless, mobile, intrusion detection to name a few.

Measures are key to the framework. Measures will be used initially to establish where the practice is with respect to each policy area. The most important aspects are the kind of measures adopted and how practical and useful they are. As discussed earlier, the current guidelines of the GPCG do not go far enough in terms of providing measures that are aligned to 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 set by law in respect of who are the legal custodians of information in a practice. A review of each practice needs to determine how well this aligns to what is actually happening in a practice and so this is 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 the assigned 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 type of important 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. Indeed this is a distinguishing feature of our definition compared to others. In many ways the element of

continuous improvement is the most important aspect of a governance framework because it doesn't matter where a practice is at, the framework allows for the prospect of improvement and so breaches, weaknesses or failures become opportunities for improvement within a controlled framework.

Accreditation system
Whilst the existence a governance framework is clearly a critical success factor, it's availability in itself is not likely to be a sufficient incentive for most practices to adopt it. An accreditation is required to motivate practices to comply. The idea and use of accreditation systems is not new in Australia and indeed accreditation systems have been successful in recent years in general practice across a range of compliance activity.

HOW DO WE GET THERE?

Firstly, widespread acceptance of the need for an information security governance framework along the lines described above needs to take place. As discussed earlier most practices in Australia are not operating at a standard necessary to ensure full patient confidentiality. These risks and threats are very real and it is only a matter of time before embarrassing media items appear. Furthermore there is in many quarters a general lack of awareness of what standards can and should be achieved and under what timescales. So work needs to be done in canvassing key decision making groups such as NEHTA, the RACGP and the Australian Medical Association to convince them of the need, viability and dangers if not undertaken. Linked with this is the need to provide incentives to general practices (as small businesses) to embark on this. In recent years Practice Incentive Payments (PIPs) have been successfully used as an instrument in encouraging uptake of a variety of activities in Australia (Medicare, 2009).

The role and involvement of the GPCG is pivotal here. Their earlier work in 2004 (GPCG, 2004a; 2004b) recognized the need for guidelines. The substance of this paper simply builds on this work since it is argued that the original guidelines did not go far enough in certain important ways. The existence of the GPCG and its current network is an important mechanism for dissemination of the governance framework.

In one sense the governance framework can be seen as a 'training package' for general practices. However, the amount of training required to roll this out across Australia requires the involvement of the existing channels of GP networks and Divisions who traditionally have provided training to practices. Clearly this should only happen once the governance framework has been tried and tested to a sufficient degree.

Current research activity involving a doctoral student centres around developing the detail of the framework and then testing it using an action research framework. As each section of the framework is completed action research activities are carried out in General Practices throughout Western Australia to verify the structure and completeness of each section. Due to the complexity of the research problem, action research is seen as a most suitable research approach as it permits a flexible goal oriented approach to solving difficult problems. For example, the area requiring most time and attention is in developing measures. Work done by Williams (2008) has 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. However, it is a problematic to identify simple useful metrics that 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 metrics need to be understandable to doctors and other practice staff for true governance to occur. After all, they are not typically ICT experts. Secondly there is a real danger that the number of metrics and benchmarks required will be such as to make the whole process unviable. So here the focus in defining the framework has been in asking what is the minimum set of measures required to achieve the goals of this framework. Achieving the right balance is critical to the success of this program and is the subject on ongoing research.

Lastly, in respect of achieving our goals, it is most important that the philosophy of continuous improvement is embedded within the program. Better to take small steps and achieve worthwhile goals in due course than to take too large steps in attempt to get there more quickly but fail because we lost the people in the process.

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.austli.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

Medicare Australia. (2009). Practice incentive program (PIP). Retrieved March 20, 2009 from http://www.medicareaustralia.gov.au/provider/incentives/pip/index.jsp

NEHTA (National E-Health Transition Authority). (2006). Review of shared electronic health records standards. Retrieved April 1, 2006 from http://www.nehta.gov.au/standard-catalogue

NIST. (2009). Security testing and metrics. Retrieved June 2, 2009, from http://csrc.nist.gov/groups/STM/index.html

Standards Australia E-Health. (2003). Information security management: Implementation guide for the healthcare sector. Retrieved June 2, 2009, from http://infostore.saiglobal.com/store/Details.aspx?DocN=AS974265969956

Williams, P. A. H. (2007). An Investigation into Information Security in General Medical Practice. PhD thesis. Edith Cowan University. Western Australia.

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

COPYRIGHT