2008

Trust me. I am a Doctor. Your records are safe

Patricia A. Williams
Edith Cowan University

Craig Valli
Edith Cowan University

DOI: 10.4225/75/57b6528934760
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.

Trust me. I am a Doctor. Your records are safe…

Patricia A H Williams
Edith Cowan University,
trish.williams@ecu.edu.au

Craig Valli
Edith Cowan University
c.valli@ecu.edu.au

Abstract

Primary care medical practices in Australia have been identified as a profession in need of assistance with information security practices. Whilst guidelines exist, there is little assistance in an accessible and easily implemented form for medical practices. This research presents the preliminary findings of a study which advocates that information security practices can be improved using a capability operational framework which is contextualised to its target environment.

Keywords: Medical information security, primary care, capability maturity model, SQL,

INTRODUCTION

Increasingly medical practitioners are either being encouraged to use information technology to make their businesses more efficient and accountable. This impetus for adoption of information technology into modern medical practices comes from several vectors. In the case of Australia, the Australian Federal government has either mandated or provided significant financial incentive for medical practitioners to modernise their practices by installing medical information systems (Australian Health Information Council, 2004). Similar schemes are also to be found in other nation states around the world including The Netherlands, UK and USA (Blobel, 2004; Hillestad, Bigelow, Bower, Girosi, & al, 2005; Watson, 2006). In addition to government forces requiring a move into information technology, many of the medical supply and medical service companies are following suit. Whether it is physical goods such as pharmaceuticals or for the provision knowledge such as test results for pathology or x-ray, many of these suppliers increasingly are requiring ordering and delivery of goods and services via electronic systems that are accessible via the Internet.

A result of this IT trend, medical practices are now availing themselves of broadband technologies and IT systems such as SQL enabled medical practice/client management databases to meet these demands. There is little argument that information systems can garner significant cost savings and strategic advantage for any information dependent organization. This cost saving is principally in the timely delivery and storage of information for legitimate purposes or use by the organisation (Commonwealth Department of Health and Aged Care, 2000).

One of the prime motivators for moving to the ubiquitous use of medical records in digital form is one of cost and the quality of care delivered for the cost. Traditionally medical records have been kept as paper based indexes, often with records held in filing compactors being the dominate feature within a medical practice. These paper records were offline in the true sense of the word. If anyone wanted to obtain the medical record, they had to have physical access to the filing cabinet or compactor to obtain the records. Furthermore, to take a copy of the file one had to either copy notes from the file to a notepad by hand or had to have access to a photocopier, or simply purloin the whole record file. Some of the problems intrinsic to copying the medical information in this manner is that unless the filer is organized it could be could be difficult or time consuming to locate information initially. If the information is not organized alphabetically or by incident, or uses chronological placement of information within the file locating the exact piece of information could take considerable time. The increased time makes the threat of discovery escalate considerably. This means that such a breach is a high risk activity for an outsider but is a profile well suited to insider malfeasance. However, the insider still runs the risk of discovery either in commissioning of the breach or egress of the information across the physical practice boundary. Unfortunately, whilst technology has moved on many of the work practices and trust in the "system" have not (Williams, 2008b). This paper is reporting on preliminary research into the information security awareness and attitudes of medical practitioners within Perth, Western Australia.

THREATS TO THE MODERN MEDICAL INFORMATION SYSTEMS ENVIRONMENT

Most medical information systems contain customized SQL database applications that run on specialized and dedicated server architectures. These databases are normally accessed by client PCs distributed across a network. These typically use Ethernet within the physical confines of the medical business and sometimes connected to wireless. Furthermore, these networks are increasingly being linked to the Internet via broadband connection such as ADSL with access speeds as high as 24Mbits per second.

The infrastructure and operating environment that these systems operate in are relatively complex in computing terms and some exploration of the attendant risks for medical practices in particular will be undertaken in the following sections. Firstly, there is typically a SQL database server containing the client databases which hold the digital records of the patients. These records not only record textual data but may also contain scans, diagnostic results and graphical images of patients. These databases need to be maintained, patched and secured against a large range of threats requiring highly specialized skills. Such skills are nearly always beyond the scope and capabilities of IT support mechanisms within medical practices. The SQL database engines themselves are vulnerable to exploit and there are many documented instances of this on computer security sites such as CERT, AusCERT and vendor specific sites such as Microsoft or Oracle.

What further complicates the issue for many medical practices is that these medical applications are highly specialized and therefore are generated often by boutique or specialist developers whose primary focus is the generation of a competent medical records system, and not security. Hence, the applications themselves may contain serious security flaws resulting in exploit that could allow escalation of privilege either within the database or the underlying operating system. Many of these potential exploits due to the low profile of many of these companies may go undetected for considerable lengths of time (Valli, 2006).

A broadband connection brings many advantages to the user including increased speed of download and the ability to search and work faster for instance. However, these same capabilities also work to aid an attacker. In the same way that a legitimate user accessing the system can download information up 100 times faster than conventional analog modems, so too can attackers send and receive at increased speeds. The greater use of bandwidth across the Internet connection allows an internal or external attacker to hide their attack within bigger data streams than is possible with conventional analog modems. What makes medical practices high-value targets is the type of personal data they store. For instance, personal records of infectious disease or before and after photography of cosmetic surgery may be valuable to malicious or financially driven attackers, or even the media. Some groups may want to access patient medical histories for informing employment or insurance prospects. It is far easier for a malicious insider to readily re-transmit this data at broadband speeds on the Internet than the conventional methods of physically accessing and duplicating the physical asset.

As well as traditional viruses and worms, there is an increasing use of targeted spyware programs. Unlike conventional viruses and worms these spyware programs are specifically built to extract confidential data from systems such as passwords, to enable an attacker to compromise a system at will. This emergent trend is worrying because unlike previous malware vectors its purpose is not wanton destruction of systems for fun but specific targeted activities for potential profit through theft or fraud.

Another potential vulnerability has been a result of the massive expansion in the growth of flash memory technologies such as USB memory sticks, SD memory sticks, portable storage and playback devices such as IPOD, MP3 players. Staff in medical practice regularly bring these devices into their work environment with little if any observation or auditing of activity. USB memory sticks can be purchased that are 16 GB in raw storage capacity for less than $80 and are small enough to be readily concealable. For example, it could be possible to store all of the medical records from a sizeable practice on one stick using a simple SQL database ASCII text file dump routine that contains SQL queries and table constructs for the whole database. Similarly, saving all word processing documents in text format and storing them on the stick is possible. Detection of such activity would be beyond most medical practices and in fact many IT enabled enterprises. One of the other major problems is recognition that these devices are capable of carrying computer related data. For instance, someone

walking out of an organisation with an iPod around their neck does not send the same suspicious signal as the same individual carrying a handful of CDs or medical files.

Another attack vector that was not possible, or was more problematic, to achieve with paper-based records is that of alteration. It is a reasonably difficult process to modify an x-ray film, however for its digital equivalent it is not. Likewise alteration of digital test results is a relatively trivial task as many of these are sent as e-mail which are often saved as text files which can be readily manipulated.

Incorrect disposal and sanitisation of storage media has found to be a significant problem in numerous studies and medical information systems are not immune to this threat vector. Some systems are sold unformatted or in a readily recoverable state, with little data recovery skills needed by the perpetrators. This problem is further exacerbated by auctions and sellers of this equipment advertising it as coming from major hospitals, making the targeting of these easier for would be criminals (Valli, 2007).

It is well documented in the computer security literature and surveys that insiders are a significant risk to systems integrity. The other alarming trend is that inside attacks are often the most successful and damaging in terms of money and loss of reputation. This is typically as a result of the insider having intimate operational knowledge that an outsider must either socially engineer and extract from the organization or bypass in the case of security countermeasures. Medical systems are no less vulnerable to these types of attacks as mentioned before due to the nature of the material they store may in fact be a high value target.

These are just some of the significant threats that are faced by modern medical organisations. While the research may not specifically examine each of the risks outlined previously it provides a background to the complex IT security environment in which medical practices now operate.

A little knowledge is a dangerous thing

In 2005 the Royal Australian College of General Practitioners (RACGP) and the Federal Government commissioned a series of security guidelines for use in securing medical practices (General Practice Computing Group, 2005; Schattner, 2005). Not only do these guides contain patent errors, they are trite and are lacking many hallmarks of good computer and network security. For instance, the information provided on ports is incorrect and thus setting up systems using such information can unknowingly create vulnerabilities.

There is little mentioned of monitoring, cycles of audit and review to mention a few. It is conceivable that review of these documents was performed by people not sufficiently informed about security and the documents do not demonstrate expertise beyond a basic understanding of the content discipline. The reverse of this situation should be seriously considered to point out the relative absurdity. So, would it seem reasonable that colleagues in the computer and network security professions receive government funding and should be writing guides on general medicine, and distributing them for serious use by computer and network professionals to perform preventative medicine for all their customers? The simple answer is no.

RESEARCH DESIGN

In light of the problems identified in the application of security measures by medical practices, based on previous work by the authors, it was anticipated that the operational framework would be able to assist in practical and measurable improvement in security practices (Williams, 2007). Such improvements must be implemented at a pace the medical practice can accommodate. The aim of the research was to assess the validity of a capability assessment operational framework (Figure 1) in the context of general medical practice information security. This was achieved by developing an experimental set of security capability measurements and testing these against actual current information security practice. The framework also allows for identification of potential improvements. The second part of the research will be to reassess the information security practices of the research participants to see if any changes are observed.

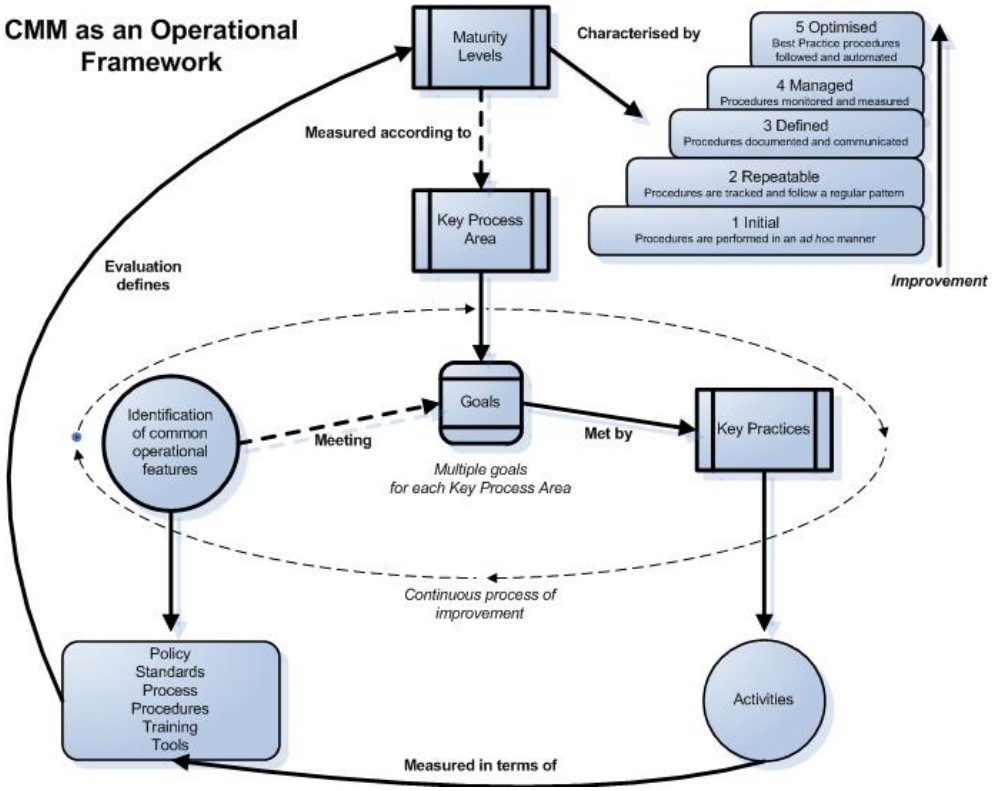

Figure 1: Capability assessment operational framework (Williams, 2008a).

Action research is used as the overarching methodology because as it encompasses: assessment of the current situation; information gathering and reflection on the intervention framework; iterative action and reflection to modify the framework; and the development and testing for sustained change. Using a sample of general practitioners in metropolitan WA, it is anticipated that approximately twenty participants will be required for the initial data collection. To date four have been sampled and assessment of these interviews will drive additional data collection if necessary.

The initial cycle involved researching and developing an experimental set of capability assessment criteria for specific security activities using the capability assessment operational framework. In addition, specific security breach scenarios were developed to assist in the measurement of current security practice and awareness, together with associated interview questions. The areas of security breach targeted were policy, backup, malware, intrusion detection and wireless.

The second cycle was initial data collection using four participants using the capability assessment criteria, scenarios and interview. Analysis of these results and subsequent assignment of capability level is currently being performed. This cycle will establish an existing baseline from which to measure actual change. The reflection stage of this cycle will include examining the data to see how well the assessment criteria fitted the real-world situation assessment and may result in improvement in the capability assessment procedures.

The third cycle will provide feedback to the research participants identifying specific improvements to progress from their current capability level to a higher one, and practical guidance on how to implement these.

The final cycle will also be data collection to reassess the new level of capability using the same criteria, scenarios and interview methods, after a period of three months. Assignment of capability level will then be re-evaluated. The reflection stage of this cycle will form the evaluation of the capability framework.

The interview data will be transcribed and QSR Nivo qualitative analysis software used to identify significant themes contributing to or inhibiting security capability improvement. Further, a comparison

of quantitative capability assignment levels will be undertaken to evaluate any change in security capability of the research participants.

RESULTS

The initial results of the survey indicate that the security situation of participant medical practices is similar.

- Most of the practices lack appropriate security policy. For instance, basic measures such as password maintenance are virtually non-existent.
    - *"Staff have individual passwords.* [But no policy on passwords]. *They can't get into anything they shouldn't. Staff are not forced to change passwords, but they can be changed if we want to";* and
    - Are your passwords changed regularly? *"Not our normal one to access the computer system we don't. Only the email ones get changed about every six or seven weeks"*.

- All lack training of staff and awareness in security measures
    - *"No training, sure firewalls are in place, runs off the server. No need for training in it."*

- No participant practices have ever undertaken a security risk assessment.
    - *"Not aware of this having been done, but I have every faith that the IT company* [contractors] *have done so"*
    - *"The only time we assess – well with the new system we don't have to do it at all. On the old system we used to have to do backups and all sorts of things like that, but now we don't touch it at all. It's all done automatically. It just sits out there and churns information into the system as it happens, I think"*.

- Most believe that complying with the RACGP accreditation standard means they are fully secured. Do you think your current security practices are sufficient in the practice?
    - *"To be honest, as I say I haven't had even been through the list yet, but I would probably need to look at it for accreditation";*
    - *"Yes. Other than ethical responsibilities, as the practice manager I know the legal responsibilities to maintain all records, and the backup is offsite in case of fire"; and*
    - *"I think they're very good"*.

- No participant practices have intrusion detection systems (IDS) they are aware of, and some thought a firewall was an IDS.
    - *"We have a firewall and I think its documented in the disaster recovery section of the manual"; and*
    - *"I imagine Trend* [software application] *would tell me that, wouldn't it? My understanding is that it is the top of the water for network environments – and it's the one that was recommended* [by the contractors]".

- All believe they are well secured.

- Specific security activities, such as backup, are undertaken but rarely checked. Further, knowledge of monitoring and necessity for media rotation is poor.

- All participants use external contractors for maintenance of their networked systems and rely on them for security, mostly without knowledge of what these measures are.

- None of the practices use wireless networks or devices.

DISCUSSION

The preliminary results are consistent between practices. There are several aspects of security failure that are clearly evident, even at this early stage of the research.

The area of basic security procedures, starting with policy, is severely lacking. This is an area that can be addressed easily and rapid improvement could be observed as policy forms the cornerstone of all

good security practice. Further, the lack of staff awareness and training in security purpose and implementation is a straightforward issue to address. Of more concern, which arises from a lack of awareness, is the omission of security risk assessment in any form, and indeed the lack of acknowledgement that it is an essential component of effective security. The areas identified at the first level of security, namely policy, training and risk assessment, can be uncomplicatedly addressed using the capability operational framework and its associated matrices of activities.

In regard to the specific security activities the following needs to be considered:

- intrusion detection appears to be an area of misconception and limited knowledge;
- backup activities are undertaken however management of this task, including monitoring and verification, could be significantly improved;
- malware is handled automatically for all practices although the level of knowledge of malware management is again poor, with most being left to the third party IT contractors; and
- wireless is avoided due to the perceived inherent risks.

Further, since there is a tendency towards outsourcing IT related activity, over reliance on third party staff without knowledge of what tasks they undertake is another area for concern. In addition, no security checking of contracting staff is undertaken, nor any conditions imposed in terms of confidentiality as would be expected of other staff in contact with patient records. This indicates a major flaw in security, as the contractor has open, authorised access without the same security control measures placed on other staff. Practices seem unaware of such potential vulnerabilities.

Another area that may require further investigation is in making practices aware of the limitations of assuming the RACGP accreditation will provide them a total security solution and one in which they can use as a defence for poor security practices. The present guidelines need reviewing in light of the advances in technology and acceptance of generally poor security implementation practices.

CONCLUSION

The results, whilst preliminary, confirm previous research and indicate that there is opportunity for major improvement in information security practices in primary care medical practices. This research aims to prove that an operational framework can promote improved security practices through the contextualisation of specific security activities to a given environment. The structure of the operational framework using the activity process, procedures, training and tools allows recognition of the requirements to progress from one level to a higher level, and thereby assisting in the identification of the critical success factors. A further benefit of the research is the ability to link specific information security capability criteria to professional standards. In the case of medical practices this refers to the Royal Australian College of General Practitioners (RACGP) accreditation standards which are used for official approval of general practices. This type of capability assessment tool has not been developed for medical practices before, as currently only checklists are available. The tool will provide practical assistance in measuring capability and in identifying realistic improvements in security practice.

This study will provide a baseline for further research into the capabilities of primary care medical practices to assess and improve their own security practices. Since primary care medical practices also effectively operate similar to small business in Australia, it is envisaged that this security capability assessment may be transferable to other areas of the medical profession, such as psychology, medical specialists and pharmacy.

REFERENCES

Australian Health Information Council. (2004). About AHIC. Retrieved 13 August, 2005, from http://www.ahic.org.au/about/index.html#terms

Blobel, B. (2004). Advanced EHR architectures - promises or reality. In B. Blobel, G. Gell, C. Hildebrand & R. Engelbrecht (Eds.), *Contributions of Medical Informatics to Health: Integrated Clinical Data and Knowledge to Support Primary, Secondary, Tertiary and Home Care* (pp. 73-78). Munich, Germany: IOS Press & European Federation for Medical Informatics.

Commonwealth Department of Health and Aged Care. (2000). *The benefits and difficulties of introducing a national approach to electronic health records in Australia: Report to the Electronic Health Records Taskforce*. Adelaide, Australia: Flinders University.

General Practice Computing Group. (2005). *Medical practice network security: Firewall tutorial*. South Melbourne, Victoria, Australia: Royal Australian College of General Practitioners.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., & al, e. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings and costs. *Health Affairs, 24*(5), 1103-1107.

Schattner, P. (2005). *The GPCG computer security self-assessment guideline and checklist for General Practitioners*. East Bentleigh, Victoria, Australia: Department of General Practice, Monash University.

Valli, C. (2006). *SQL Injection - Threats to Medical Systems; Issues and Countermeasures.* Paper presented at the The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'06 - The 2006 International Conference on Security & Management, Monte Carlo Resort, Las Vegas, Nevada, USA (June 26-29, 2006)

Valli, C. (2007). IT Sharps: Disposing of your IT medical waste. In H. R. Arabnia & S. Aissi (Eds.), *Proceedings of the 2007 International Conference on Security & Management*. Monte Carlo Resort, Las Vegas, Nevada, USA (June 26-29, 2007) USA: CSREA Press.

Watson, N. (2006). Patients should have to opt out of national electronic care records. *British Medical Journal, 333*(7557), 39-43.

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

Williams, P. A. H. (2008a). A practical application of CMM to medical security capability. *Information Management & Computer Security, 16*(1), 58-73.

Williams, P. A. H. (2008b). When trust defies common security sense. *Health Informatics Journal, 14*(3), 211-221.

COPYRIGHT