Information Governance: A Model for Security in Medical Practice

Patricia A. H. Williams
School of Computer and Information Science
Edith Cowan University
Joondalup, Western Australia Australia
trish.williams@ecu.edu.au

ABSTRACT

Information governance is becoming an important aspect of organisational accountability. In consideration that information is an integral asset of most organisations, the protection of this asset will increasingly rely on organisational capabilities in security. In the medical arena this information is primarily sensitive patient-based information. Previous research has shown that application of security measures is a low priority for primary care medical practice and that awareness of the risks are seriously underestimated. Consequently, information security governance will be a key issue for medical practice in the future. Information security governance is a relatively new term and there is little existing research into how to meet governance requirements. The limited research that exists describes information security governance frameworks at a strategic level. However, since medical practice is already lagging in the implementation of appropriate security, such definition may not be practical although it is obviously desirable. This paper describes an on-going action research project undertaken in the area of medical information security, and presents a tactical approach model aimed at addressing information security governance and the protection of medical data.

Keywords: Medical informatics computing, computer security, security measures, data security, action research.

1. INTRODUCTION

Like most organisations, medical practice is increasingly dependent on IT systems and data in electronic form. The information used is both administrative and clinical in nature. In addition, like e-commerce, the boundaries for health provision are becoming blurred. Where once the family doctor was the main provider of healthcare, the services have become distributed (Williams and Mahncke, 2006). The increased push for shared electronic health records compounds the security issues in this environment. There is a need to ensure a secure and trusted environment for the use and transference of sensitive personal information. Von Solms (2000, 2006) describes the 'waves' of information security as technical, management,

standardisation and most recently information security governance. Whilst the corporate world has faced these waves head on, the medical profession has been slow to progress past the first wave. The existing tactical policy approach taken by organisations to information security is becoming inadequate as it does not reflect the changing electronic environment and its attendant risks, nor does it address the increasingly important issue of accountability. This research confirms the slow progression through Von Solms' waves, and provides an overarching practical model for medical practice to follow in order to secure their medical information, and thus generate defensible information governance.

2. BACKGROUND

Information governance is a relatively new idiom and echoes corporate governance in its concern with accountability and fiduciary duty. Essentially it encompasses integrity, including audit and control, risk management and compliance. Similarly, information security governance extends the definition of information security (confidentiality, integrity and availability) to incorporate the legal and regulatory aspects of the context in which the IT security is used. These definitions imply accountability at the highest level of the organisation. Well known corporate failures in this area include Enron and more recently WorldCom, and have given rise to legislation for senior management responsibility such as the Sarbanes-Oxley Act (Sarbanes-Oxley, 2002). These examples show that directors and CEOs are ultimately responsible for the safety and security (in all its facets) of information in an organisation (Von Solms, 2006).

In the face of strong penalties for violations of corporate governance directives, it is time that organisations paid more attention to the protection of information assets. Understanding the liability that organisations are open to is a strong motivator for change in regards to security practices. In the medical field, such protection has been encapsulated in legislation in some countries, for example in the Unites States there is the Health Insurance Portability and Accountability Act (HIPAA). However, other countries such as the United Kingdom, the European Union and Australia do not have such defined legal statutes and rely on national privacy laws (Heiser, 2004; Hinde, 2003).

Similarly, to fully appreciate how security contributes to governance, the difference between information security management and information security governance must be understood. Information security management is wholly contained within information security governance. It is the process of attempting to comply with legal and professional requirements, which is a key part of information governance. It has been a criticism that "information security is often treated solely as a technology issue, when it should also be treated as a governance issue" (Business Software Alliance, 2003, p.2).

In the medical arena, the purpose of information security governance is to

protect all health-related information to ensure confidentiality, integrity and availability. However, more than this it is to ensure business continuity and mitigate the risks of litigation by demonstrating and proving best practice and robust procedure compliance. The process of governance must be integrated with other standard processes if it is to be effective. A complementary review of ISO17799/AS7799, ISO27001, HIPAA and other relevant security and medical security standards can be found in Williams (2006c).

Surveys have shown that information security problems arise frequently from human negligence rather than intentional attack (Cosgrove Ware, 2004) and at the same time there has been a decline in the adherence to security standards. Approximately 50% of intentional attacks are from current or past employees, yet statistics in security show that over half of security breaches are never reported. The 2006 Australian Computer Crime and Security Survey suggests that it is the users' attitudes and resulting behaviours towards security practice that requires the most attention and pose the greatest challenges for organisations today. The survey reports that less is being spent on security than in previous years, yet still only 10% of organisations consider that they manage their computer security at an acceptable level. Concurrent with this is a decline in the adoption and integration of IT security standards. Many security incidents can be attributed to a lack of appropriate protection as a result of inadequate staff awareness of security procedures and a poor security culture. These surveys suggest that whilst increasing security awareness and implementing measurable security activities is challenging, they may have the greatest protective effect on security. In medical practice, these security issues have been shown to be greatly underestimated and therefore it is imperative that the security research provides assistance to this area of society (Holzer & Herrmann, 2002; Williams, 2005).

2.1 Existing Information Security Governance Frameworks

Information governance and information security governance are immature concepts and hence there is limited literature on the subject and even fewer models and frameworks. The literature that does exist views information security governance as a strategic function.

Moulton and Coles (2003) proposed that security governance should comprise strategic objectives for security with strategies to meet these objectives, identification of responsibilities and practices together with the associated resources management, risk assessment, and regulative compliance. In addition, they suggest that information security governance is "the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems" (Moulton & Coles, 2003, p.581). However, this definition specifically omits the audit function, the operational security activities and future development. It clearly focuses on applying information

security governance at a strategic level.

In comparison, Posthumus and von Solms (2004) also classify information security governance as an executive management responsibility. Their work presents a framework for how information security can be dealt with at the strategic level. The framework includes a 'direct and control' view of information security governance, comprising both governance and management responsibilities. This sees executive vision, strategy, and policy in governance as 'direct', and the implementation and reporting from the management side as 'control'.

From a software security viewpoint, the National Cyber Security Partnership in the US also proposed a framework specifically defining information security governance in terms of the roles of executive management (Business Software Alliance, 2003; Entrust, 2004; National Cyber Security Summit Task Force, 2004). This approach centres on business drivers, responsibilities and metrics, and defines the actions needed to be taken by management to meet governance through engagement of strategic management. Other organisations such as the IT Governance Institute have also published resources that specify "information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organisation's response to them" (IT Governance Institute, 2006, p. 8).

The existing frameworks indicate that governance is a management issue and should be initiated and controlled from this strategic organisational level. The authors identified as the major contributors in the field of information governance all indicate that the frameworks have been developed to provide assistance in meeting information governance. Further, they acknowledge that more support is required to interpret the directives at a tactical and operational level.

3. METHODOLOGY

This research is part of an information systems based, action research project. The objective of the research is to formulate practical models of assistance for primary care medical practices to improve their security practices. Action research was chosen as the overarching methodology because its cyclic nature supports investigation and intervention in real-world situations (Baskerville, 1999; Baskerville & Wood-Harper, 1996; Dick, 2002; Susman, 1983; Whitehead & McNiff, 2006). Action research is "widely cited as an exemplar of a post-positivist social scientific research method, ideally suited to the study of technology in its human context" (Baskerville and Wood-Harper, 1996). It allows for situational assessment, question raising, planning, fieldwork, and analysis/reflection of interventions leading to sustainable improvement.

It is imperative to involve those who would use and be affected by the research, particularly in the medical domain where there has been a natural opposition to investigation into, and challenge of, current processes (de Dombal, 1993). Action research is one research methodology which fits the primary care environment where both technological and human factors are present, and where strong emphases on quality solutions are essential. Further, it has been shown that collaborative research between researchers and participants works well in the medical context where the purpose is to improve the adoption of appropriate research findings (Hoddinott & Pill, 1997). Such qualitative research, as action research principally is, can assist in understanding the processes and capabilities of individuals in the health setting, and promoting sustainable change (Muecke, 1997). A detailed discussion of the research process can be found in Williams (2006a).

The research initially employed an exploratory pilot study, followed by in-depth semi-structured interviews with primary care medical practices. The pilot study aimed to investigate what issues were present in medical practice in the use of electronic information. The research subjects were single and group practitioners in private primary care practices in Australia. The results of this study indicated that security and trust were significant issues in the use of electronic information. After this initial action research cycle, the results were critically reviewed and, consistent with the evolutionary nature of the action research paradigm (Dick, 1993), further literature investigation was carried out. This led to a refinement in research objectives and the initial development of the model presented in this paper. Further, it motivated the development of a security specific questionnaire based on the four competing security factors: **demographics, actual practice, issues and barriers,** and **practitioner perception** (Figure 1). These distinct competing factors in security were chosen because of their importance to the existent social information system and to the technological solutions that may be in place.

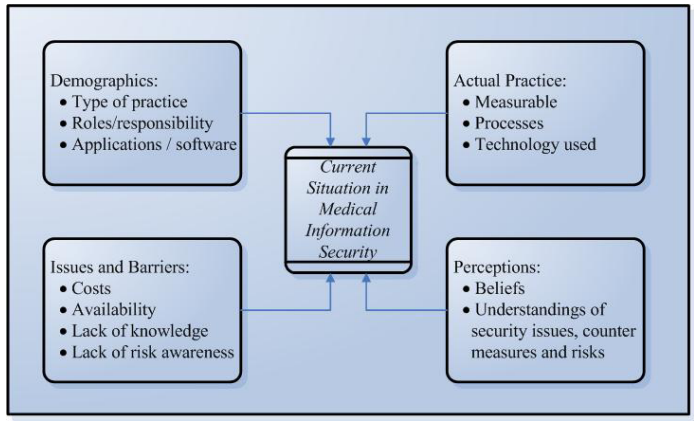

Figure 1. Competing factors in information security (Williams, 2006a).

Information security research is often seen as one of the most intrusive and sensitive types of information systems research. There exists a general mistrust of any person outside an organisation attempting to gain information about the security and security practices (Chang & Ho, 2006). Several researchers report that to gain meaningful data in security it is preferable to use a small sample and build relationships with those participants (Chang & Ho, 2006; Kotulic & Clark, 2004; Straub & Welke, 1998). Furthermore, to effect change using action research, trust needs to be fostered with the participants in order to undertake intervention in the target environment as the participants are inclusive in the research. For these reasons the interviews were conducted with group medical practices in Australia and the UK, with whom a relationship could be developed. Each practice has a networked medical records and administration system with access to the Internet. The participants share information within the medical practice and seek information from the Internet. The UK practice also shares information over the UK NHS Spine. Following the data collection and analysis, the model was refined.

4. RESULTS

The results are a snapshot of the extensive qualitative interview data collected. They provide examples of key factors in relation to responsibility, legal requirements, and improvement in information security. All practices have a networked computer system for administration and clinical records. Little delineation of security roles was apparent. In relation to *responsibility* and the question 'Who is responsible for maintaining the security of your electronic information?' respondents reported:

> "Well I suppose it has to be me [as Practice Manager]…although because of the connections that we have to the [NHS] Spine, now I don't know how that changes my roles as far as security, as I do not really have any remit to control them"; and
>
> "At the moment it's me [doctor] and then later on I will designate it to my wife who is trained in IT so she can handle that".

The interviews revealed identical approaches to security, which was reliance on existing security measures provide by the application software and some influence of profession accreditation requirements. In 'actual practice', whilst policy was seen as important and acknowledged as a necessity, formal written policy was either non-existent or not well developed. Secure access was handled almost exclusively by the facilities available in the software application packages used. The most obvious exception to this was the backup procedures, which were well defined and usually formally written down.

Respondents revealed little explicit knowledge of the legal responsibilities associated with security of electronic information. It should be noted though that this does not preclude interviewees having tacit knowledge of the required

obligations. In relation to the *legal requirements* and the question 'Are you aware of the practice responsibilities from a legal perspective in relation to the security of your electronic information?' respondents said:

> "We get people to sign a confidentiality agreement";
>
> "I know it's under some sort of act but I can't quote on it. I just know it has to be as confidential as possible and I'm sure that's all they [laws] are trying to say"; and
>
> "There is an awareness. I don't know the detail. I know it's the practices' responsibility to ensure the confidentiality of all patient related information. There is a legal implication on me being the administrator of the records, to ensure that those are all protected. I wouldn't know the detail of the legalities".

In regards to security perception, there was a consistency between practices where all interviewees thought that the application software used provided sufficient protection in terms of security. Further, although some auditing and security metrics are recorded, albeit automatically by application software and the operating system, the interviewees revealed that these metrics are not monitored. Such audit data could however partially fulfil some requirements of information governance and could be used to review and inform security processes. They may also be a key factor in the process of risk assessment. Consequently *improvement in information security* was investigated through the following questions:

1. What do you think constitutes good information security practice?

   > "I think it has to be up to the individual who's doing it, I think you've just got to be checking it all the time I think that's the only security you've got isn't it you can't rely on the computers to do that for you so I think it's monitoring constantly"; and
   >
   > "We have to have a robust policy that is clearly communicated to all people who use the building to serve the patients".

2. What do you think would improve information security in your practice?

   > "I think we have to educate the staff more, especially the ones who are not computer literate, that would definitely improve security"; and
   >
   > "We don't monitor [security] its just too much time and human resources"; and
   >
   > "I think an alarm system for the building, the protocols for email and the internet, would be something I need to look at sooner rather than later. That would cover the physical side and the educational side".

3. What are the issues in implementing security in the practice?

   "The biggest issue was the need to look at it. It's now on the strategic document and there is now a recognition that we need to do something. Knowledge is an issue for me. Where to gain that knowledge is also an issue"; and

   "We have some user issues, i.e. the capabilities of some of the staff. They vary completely from the new partner who is really switched on, to the one who used to be a typist who has come on board as an excellent receptionist".

In summary, the data collected identified the following issues:

- No clear delineation of responsibility for security;
- Risk assessment is not undertaken;
- Policy is usually 'ad hoc' and not in written form;
- Security measures are often implemented incorrectly or poorly including monitoring of existing measures;
- The capability and understanding of staff is in question in regards to security;
- Education of staff is required; and
- More appropriate procedures could be put in place.

These characteristics are key operational aspects of information assurance and governance.

Upon reflection the participants all reported that there was more that could be done but time was an issue. In addition, policy was seen as a key constituent of good information security practice. Increased knowledge and training, together with more strategic direction, were identified as important issues that needed addressing. Lastly, staff awareness and capability was seen as a fundamental gap in the security implementation at each medical practice.

5. DISCUSSION

As a result of the pilot study, a literature investigation into current security practices in primary medical care was undertaken. This, together with a review of existing information governance models resulted in the first iteration of the model. The model was further refined using the interview data collected into the 'Tactical Information Governance Security Model' (TIGS Model) as shown in figure 2. The model presented is specifically drawn using total quality management (TQM) notation as this reflects the process and function of each step in the model (Ahire, 2001). The following section discusses how the TIGS model was constructed and explains its functioning.

5.1 Model Construction

The model was derived from a synthesis of the literature and interview data using three discrete yet convergent constructs. The first constructor was a review of the literature on current information governance thinking, where it was noted that there exists a discrepancy between the compliance to information governance objectives and the operational management tasks to meet these objectives (von Solms, 2005). This is further confirmed by the interview data concerning the *responsibilities* and *legal requirements* of information security. Therefore in the top level of the TIGS model there was a need to ensure that the legal, ethical and professional responsibilities are explicitly understood. This requires that a separation of duties and identification of roles in security management are clearly defined within the medical practice. The data collected suggests that practices do not have dedicated security aware staff and that these roles are taken on by the doctors themselves or the practice manager – neither of whom are trained for this role.

The second constructor was a review of existing information security management practices. This resulted in a separation of associated processes into defined modular steps (as indicated by the dotted arrows on the left hand side of the figure 2). Usually this is termed merely 'risk assessment', which is a basic security process however it can be further refined into several tasks. In a medical application this should include:

- Identification of assets to be protected (Williams, 2006d);
- Risk assessment to obtain an overview of the anticipated threats and risks to data (Williams 2006b);
- Development of policies and procedures for those responsible for security, and other staff, to follow (Williams, 2006c); and
- Implementation of protection measures appropriate to the environment.

Whilst this delineation of tasks is adequate, it is not sufficient given the medical context. Thus, a third constructor was used. As can be seen from the data, *improvement in information security*, what constitutes good information security practices as reported by the respondents is reasonable, yet such measures are not conformed to or effectively implemented. Further, the respondents identify that capability, as well as time, are significant issues. Therefore, a capability assessment module was added to the model which can then inform and drive the subsequent procedures, protections and controls.

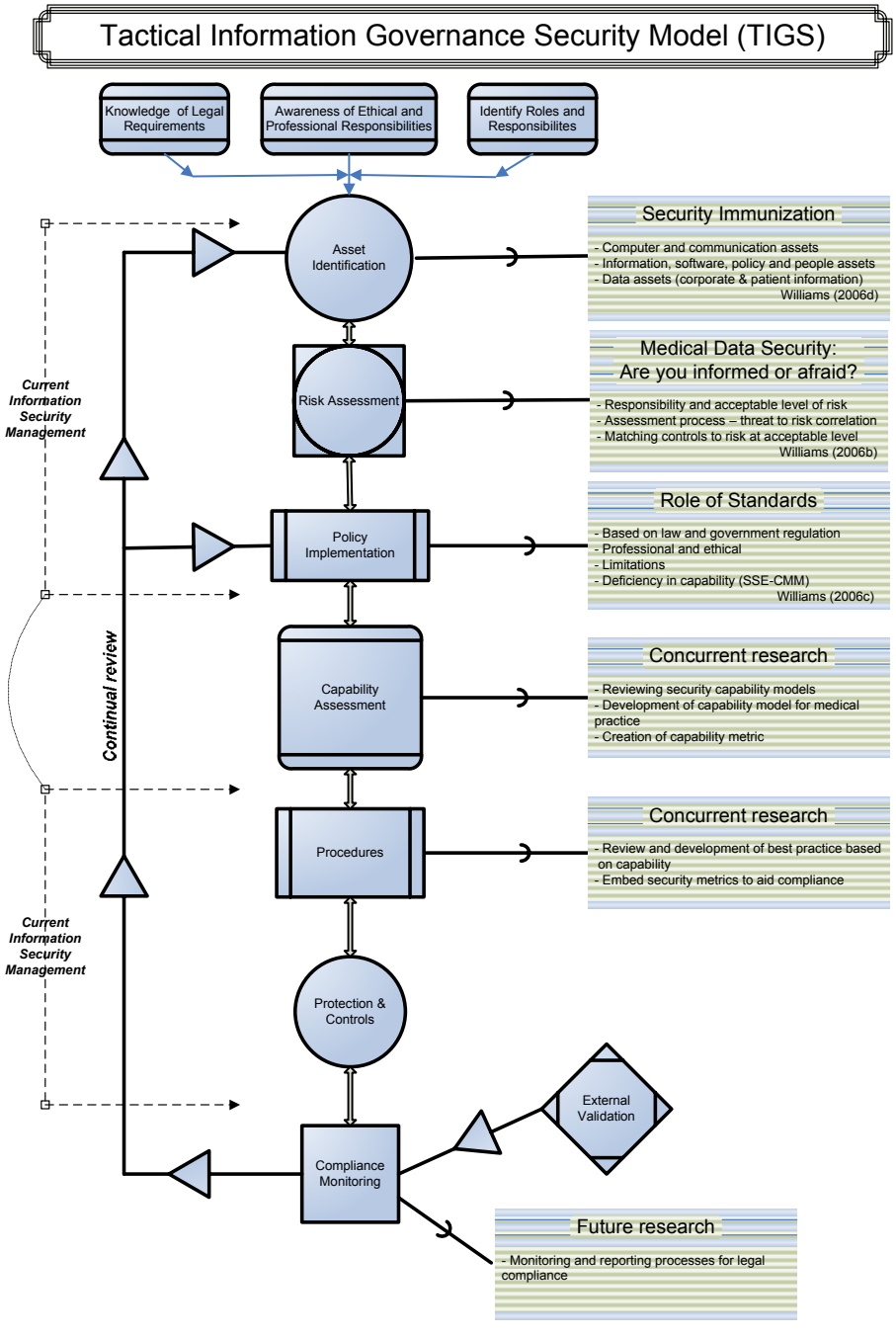

Figure 2. Tactical information governance security model (TIGS Model).

5.2 Model Function

The model specifies three prerequisites in order to make the governance process effective. These are:

- explicit knowledge of legal requirements in the use of patient and other medical data held electronically;
- awareness of ethical and professional responsibilities in the practice of medicine and in the provision of healthcare; and
- identification of the roles and responsibilities of staff and management in the governance process.

These pre-requisites provide a contextual basis for the remainder of the governance process.

The first three operations in the model are:

- **Asset identification** – this is identification of all assets of the information environment. This comprises both computer and information assets, such as hardware, telecommunications and networking equipment, software programs and operating system, human resources, and patient, management and other clinical support data. Further, practice policies and personnel intellectual property are also assets to be protected and therefore should be included (Williams, 2006d).
- **Risk assessment** - this process identifies the potential threats; matches assets to the potential threats; assesses the level of risk to an asset and the impact of the threat if it was successful; correlates the vulnerability (level of risk of a threat to an asset); and assigns control measures to each threat/asset combination (Williams, 2006b); and
- **Policy implementation** – policy is the driver for operational procedures. The policy is driven by the legal regulation, professional accreditation and established industry best practice (Williams, 2006c). Ethical considerations that may override security must also be considered.

The results of the research indicate that these three areas require substantial elucidation and explanation to enable medical practices to implement them effectively.

The next organisational function of the model is **capability assessment**. An analysis of access practices, together with the marginal delineation of the security responsibility role, reflects the trustful environment within which these are conducted. Despite some security measures being in place, the research results indicate that awareness of the security risks is minimal and that the capability of the practice to understand, and meet the legal requirements, is

equally minimal. This evidence indicates significant gaps in knowledge and execution of security practices. Thus, capability assessment is an essential component of the TIGS model. It is envisaged that this capability will necessarily be context specific and will include capability metrics for the medical practice.

Procedure development is the next key aspect of implementing effective security governance. The model specifies that procedure development should be performed to reflect the capability of the medical practice whilst still meeting the strategic intent of security requirements. To aid the evaluation of the governance process, metrics should be embedded into the resulting procedures. Further, the implementation of **protection and controls** must be consistent with capability and allow external support to enhance capability if required. This operation is dependent on the controls selected and may be technology and socially based. These may include technical education in security measure implementation and education to increase awareness of security. The final operation is the evaluation of metrics and possible external validation to meet the requirements of **compliance monitoring** and regulatory directives. It is envisaged that the compliance monitoring may be able to be embedded in the capability assessment and in the procedures used based on these capabilities. The model is seen as a continuous process rather than a discrete set of steps, and thus requires review and reiteration to be current and effective.

As the model indicates, information security management is an integral part of information security governance. This model is more inclusive than information security management, in that it focuses on validation of the process and procedures as evidentiary from a legal perspective. Yet more than this, the model is differentiated by the inclusion of a capability assessment to inform procedures development. The capability assessment model will provide a substantive security metric that is derived from original requirements for the context to which it is applied, in this case primary care medical practice. The model is designed to provide an overarching structure for improvement in security operation, implementation and execution. The modular structure of the model means that it can be employed incrementally and each module in itself may improve the overall security awareness and operations in the medical practice. It is specifically developed to be utilised by non-IT and non-security skilled medical and administrative staff, although such skilled personnel would also benefit from the model.

5.3 Model Review

The model was reviewed by five general practitioners and three security experts. Reviewers were asked whether they understood the model, their perception of its practicality, ease of implementation and possible omissions and improvements. All respondents commented that the model was

understandable, although some doctors did not fully comprehend all of the processes without supplementary explanation. Also, all reviewers indicated that TIGS was a practically oriented model and addressed an area deficient in medical practice. One general practitioner said it provides a "practical solution to increase awareness and security for patient data in General Practice, which is currently lacking" and another commented "it's very interesting to see the model like this. It is the sort of thing we don't usually try to reduce into an algorithm or a set of steps". This was agreed with by another doctor: "I think there needs to be a template. I think there needs to be an understanding of what the pathways and processes are and the requirements of compliance at a practice level".

Compliance monitoring, including the affect of outside influences such as the Government, was raised as a key area of deficiency in current practice. It was suggested that the compliance process could be linked to medical association accreditation, to ensure it meets minimum professional standards. One security expert commented that the model is focused on process and procedure and not just on technical implementation. Therefore it provides a holistic view of security within a given context. Each procedure is coupled tightly with the next, and as a result "the whole is greater than the sum of the parts". Another security expert suggested that distinguishing between the strategic and operational aspects would be the next step in implementing the model. Perhaps the review can be summed up by one doctor who commented that **"**governance is becoming more important for the patient as well as for the legal requirements. It's amazing that it has taken so long to come up with this [model] as I have been recording records electronically for over 20 years".

6. CONCLUSION

The immaturity of 'information governance' and the lack of research into its application within the security discipline suggest that there is a need to develop models of governance that can be practically applied. Medical practice has been identified as one area that to date has been sluggish in its adoption of security and is therefore open to greater security risk. The model presented in this paper provides a method for mitigation of security risk whilst meeting the requirements of information security governance within a corporate framework. Whilst it is acknowledged that information security governance should be a strategically driven process, this research proposes an applied, interventionist and tactical approach be adopted for information security governance in medical practice. This is particularly necessary given the indicated lack of security awareness and capability displayed by primary care medical practices within this study. Although the TIGS model approach to improving security in medical practice is theoretical and operational testing has not yet been undertaken, subsequent research is developing the capability assessment process of the TIGS model. Following this, the model will be tested

in several general practices in Australia and the UK. This future research will bridge the gap between the theoretical models of security and practical implementation of such models. This will ultimately provide practical guidance in improving security practices consistent with best practice and the strategic intent of information security.

REFERENCES

Ahire, S. L. and Ravichandran, T. (2001), "An innovation diffusion model of TQM implementation", Engineering Management IEEE Transactions on, 48(4): 445-464.

Baskerville, R. (1999), 'Investigating information systems with action research', Communications of the Association for Information Systems, 2, Article 19, http://www.cis.gsu.edu/~rbaskerv/CAIS_2_19/CAIS_2_19.html, 11 January, 2006.

Baskerville, R., L. and Wood-Harper, A. T. (1996), A critical perspective on action research as a method for information systems research', Journal of Information Technology, 11(3): 235-246.

Business Software Alliance. (2003), 'Information Security Governance: Toward a Framework for Action', http://www.entrust.com/resources/whitepapers.cfm, 3 July 2006.

Chang, S. E. and Ho, C. B. (2006), "Organizational factors to the effectiveness of implementing information security management", Industrial Management & Data Systems, 106(3): 345 - 361.

Cosgrove Ware, L. (2004), 'The State of Information Security, 2004', http://www.cio.com/archive/091504/security.html, 13 August 2006.

de Dombal, T. (1993), 'Medical decision making, clinical judgment, and decision analysis', in Analysing How We Reach Clinical Decisions, eds. H. Llewelyn and A. Hopkins, Royal College of Physicians of London.

Dick, B. (1993), "You want to do an action research thesis?", (An Interchange resource document No. v2.06:930507), Interchange, Brisbane.

Dick, B. (2002), 'Action research: action and research', http://www.scu.edu.au/schools/gcm/ar/arp/aandr.html, 10 June, 2003.

Entrust. (2004), 'Information Security Governance: An Essential Element of Corporate Governance', http://www.entrust.com/resources/whitepapers.cfm, 13 August, 2006.

Heiser, J. G. (2004), "The regulation of information security", Intermedia, 32(2): 29.

Hinde, S. (2003), "Privacy legislation: A comparison of the US and European approaches", Computers & Security, 22(5): 378.

Hoddinott, P. and Pill, R. (1997), "Qualitative research interviewing by general practitioners. A personal view of the opportunities and pitfalls," Family Practice, 14(4): 307-312.

Holzer, G. and Herrmann, N. (2002), 'Informatics survey for practice managers', http://www.sadi.org.au/survey/Practice_Managers_Survey_2002.pdf, 14 August, 2005.

IT Governance Institute. (2006), Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd ed.), IT Governance Institute, Rolling Meadows, IL, USA.

Jaye, C. (2002), "Doing qualitative research in general practice: methodological utility and engagement," Family Practice, 19(5): 557-562.

Kotulic, A. G. and Clark, J. G. (2004), "Why there aren't more information security research studies?" Information and Management, 41(5): 597-607.

Moulton, R. and Coles, R. S. (2003), "Applying information security governance," Computers and Security, 22(7): 580-584.

Muecke, M. A. (1997), 'Policy as forethought in qualitative research: A paradigm for developing country social scientists', in Completing a Qualitative Project: details and dialogue, ed. J. M. Morse, Sage Publications Inc., Thousand Oaks, California.

National Cyber Security Summit Task Force. (2004), 'Corporate Governance Task Force Report: Information Security Governance: A Call to Action', http://www.cyberpartnership.org/InfoSecGov4_04.pdf, 4 July 2006.

Posthumus, S. and von Solms, R. (2004), "A framework for the governance of information security," Computers and Security, 23(8): 638-646.

Sarbanes-Oxley. (2002), 'Sarbanes-Oxley Act of 2002', http://www.sarbanes-oxley.com/section.php?level=1&pub_id=Sarbanes-Oxley, 10 August 2006.

Straub, D. W. and Welke, R. J. (1998), "Coping with systems risk: Security planning models for management decision making," MIS Quarterly, 22(4): 441-469.

Susman, G. (1983), 'Action research: a sociotechnical systems perspective', in Beyond method: Strategies for social research, ed. G. Morgan, Sage, Newbury Park.

von Solms, B. (2000), "Information Security -- The Third Wave?" Computers and Security, 19(7): 615-620.

von Solms, S. H. (2005), 'Information Security Governance - Compliance management vs operational management', Computers & Security, 24(6): 443-447.

von Solms, B. (2006), "Information Security – The Fourth Wave," Computers and Security, 25(3): 165-168.

Whitehead, J. and McNiff, J. (2006), 'Action Research Living Theory', Sage Publications, London.

Williams, P. A. H. (2005). 'The underestimation of threats to patient data in clinical practice'. 3rd Australian Information Security Management Conference. Sept 30. Edith Cowan University, Perth, WA.

Williams, P. A. H. (2006a). 'Appraising information security rituals in primary care medical practice'. Sixth International Network Conference (INC2006). Jul 11-14. Plymouth, UK.

Williams, P. A. H. (2006b), "Medical data security: Are you informed or afraid?" International Journal of Information and Computer Security, 1(3): (Accepted for publication).

Williams, P. A. H. (2006c). 'The role of standards in medical information security: An opportunity for improvement'. 2006 World Congress SAM'06 - The 2006 International Conference on Security & Management. Jun 26-29. Las Vegas, Nevada, USA.

Williams, P. A. H. (2006d). 'Security immunisation using basic countermeasures'. 2006 World Congress SAM'06 - The 2006 International Conference on Security & Management. Jun 26-29. Las Vegas, Nevada, USA.

Williams, P. A. H. and Mahncke, R. (2006), "Shared Electronic Health Records: A changing landscape for security in medical practice", Journal of Information Warfare, 5(2): 61-72.

ABOUT THE AUTHOR

Patricia Williams began lecturing at Edith Cowan University in 2001 after 17 years in the medical and pharmacy computing industry. Trish has a Bachelors degree in Mathematics and Computing and a Masters degree in Computer Science. She lectures in networking, medical informatics, computer security and decision making, and has a keen interest in the development of lifelong learning and generic skills. Trish is also nearing completion a PhD in Medical Informatics and Security and has published widely in the area of medical information security.