MEDINFO 2010
C. Safran et al. (Eds.)
IOS Press, 2010

doi:10.3233/978-1-60750-588-4-651

Trust – Can it be controlled?

Debra Box[a], Dalenca Pottas[b]

[a &b] School of Information and Communication Technology, Faculty of Engineering, the Built Environment and Information Technology, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

Abstract

Trust is an important component in the security of an information system. The advent of the electronic health record (EHR) and the health information system (HIS) have raised it to greater prominence. These systems and their intended benefits are rendered less effective through a low level of trust between the stakeholders. The potential reciprocal relationship between accountability and trust is investigated. A literature study examines both concepts and their interrelationship. The accountability and audit controls provided by the NIST SP 800-53 security guide and the ISO 27799 security standard are extracted, collated and expanded to strengthen the accountability mechanisms within an HIS security program. A dedicated set of accountability controls (NIM) which is specific to the healthcare environment is produced. It is proposed that through the strengthening of the accountability function of the HIS, its level of trustworthiness may be improved

Keywords:

Medical informatics, Accountability, Security measures.

Introduction

There has been a dramatic change in the management of health information using information technology (IT) during the last decade. The adoption of the electronic health record (EHR) together with the evolution of communication mechanisms such as the Internet have enabled the transfer and sharing of clinical information. These developments have arrived with an attendant increased risk to the safety of sensitive patient information [1].

The EHR provides discernable benefits in the administration of patient care and to medical research [2]. Its use allows easier access to the patient information. The sharing of these records facilitates government health-care decision making and medical research using de-identified patient data [3]. It is seen as superior to the paper version because the information is presented in a coherent manner, can be distributed to many locations and its access rules are explicit. It is not possible to ascertain who has viewed a paper record, but it is possible to record all and any access to an EHR [2].

The wealth of information contained in the EHR, however, poses additional security risks which have far-reaching effects. It contains all the information about an individual that a thief needs to steal their identity. Medical identity theft is a growing trend but healthcare providers are more concerned about protecting the clinical information. It is protected by layers of security but similar regard is not applied to Personally Identifiable Information (PII) [4]. This contradiction was noted in 1998 by Barber and is still an issue according to [4]. Healthcare practices who fail to protect the PII of their patients risk their reputation and harm such as the loss of public trust, legal liability or damages [4, 5].

This apparent security gap affects the confidence of the patient in the usefulness of an automated Health Information System (HIS). This concern about privacy hampers the truthful exchange of information between the patient and the clinician. It is seen as a major hindrance to achieving the full potential of an HIS [6].

The importance of security is highlighted by the global proliferation of privacy and data protection legislation such as the Data Protection Directive of the European Union, the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, the Asia-Pacific Economic Co-operation (APEC) Privacy Framework and the Health Insurance Portability and Accountability Act (HIPAA) in the United States of America [5, 6].

Recent research in both Australia and the United Kingdom indicates that healthcare staff enjoy a high confidence level which results in minimal scrutiny of the HIS usage which brings a variety of possible security breaches through the improper use of access rights [7].

The healthcare environment is characterised by its co-operative nature and the trust placed in the judgement and activities of the healthcare professionals. It is an environment where security is not seen as a serious issue due to the professional status of the role players [8]. There are many factors that influence personal ethics and the fact that the healthcare personnel, using an HIS, are, in the main, members of professional bodies implies that a high level of professional trust exists. This type of trusting organisational culture acts as barrier to recognizing security threats and results in information security not being given the prominence it requires [3].

It is essential to build trust in an HIS because quality health care depends on accurate information [6]. The importance of good information within an HIS and its benefits cannot be understated. These include improved patient care and the creation of a culture of trust between the patient and

healthcare provider. As stated by Alshawi, Missi and Eldabi "after all, what is information if you cannot trust it?" [9].

It is proposed, in this research, that a high level of professional trust in healthcare environments may be controlled through a set of accountability measures. It is argued that trust and accountability are seen to exist in a reciprocal relationship and that the greater the accountability of an HIS may result in increased trust by both the users and patients. This leads to an examination of the security controls or measures themselves that are dedicated to accountability and the role they play in establishing accountability and enhancing trust. A resultant accountability control set specific to the healthcare environment is produced.

Method

A literature based approach was used to investigate the concepts of security management and control, accountability and trust. The literature study argues towards a reciprocal relationship between the concepts. The security controls that relate to the concepts of accountability and auditability were re-examined. Those controls that related specifically were extracted and collated. A resultant accountability and audit control set was produced, titled the NIM Accountability control set (NIM). This was achieved using the following method.

The following four source documents were identified as relevant to compile the NIM Accountability control set, viz:

- NIST SP 800-53. A guide to recommended security controls;
- ISO 27002, standard for IT security techniques and guide to information security management;
- ISO 27799, standard for health informatics and information security management using ISO 27002;
- Markle Foundation Connecting for Health – The Common Framework.

The NIST publications are used in this research because they are widely accepted and are freely available. They present generic guidelines that are applicable across a variety of organisational situations and their range of subjects is extensive. The ISO 277002 and ISO 27799 standards are used because they are internationally accepted and are well-known. The Markle Foundation Connecting for Health Common Framework is used because it represents an independent and unrelated viewpoint. It is the result of collaboration between various healthcare and IT professionals.

The NIST Computer Security Division has developed a variety of publications concerned with security programs and controls which encompass fair information practices, privacy principles, management and specifically auditing and accountability mechanisms. The NIST SP 800-53 covers the steps that address security control selection and includes tailoring the security controls. There are seventeen control families which have a two-character identifier unique to each family and are divided in to technical, operational and management classes. Examples include AC-Access Control, Technical Class to SI-System and Information Integrity, Management Class. The family of particular interest to this research is the AU-Audit and Accountability in the technical class [10].

The ISO/IEC in their publications ISO 27002 and ISO 27799, related to information security and health information security respectively, specifically address a security program and an ISMS and include monitoring and audit logging.

The Markle Foundation Connecting for Health Common Framework includes core privacy principles, trusted network design and accountability mechanisms [6, 11, 12].

The NIST SP 800-53 was identified as a natural starting point to define a control set for Accountability, because it specifically contains a family of controls dedicated to Audit and Accountability (AU). Thereafter, the corresponding controls in the ISO 27002 were identified, using a security control mapping tool provided by the NIST SP 800-53. It was noted that all the AU-Audit and Accountability controls, with the exception of AU-13 and AU-14, were covered. This rendered an ISO-27002-based control set dedicated to Accountability as defined by the SP 800-53.

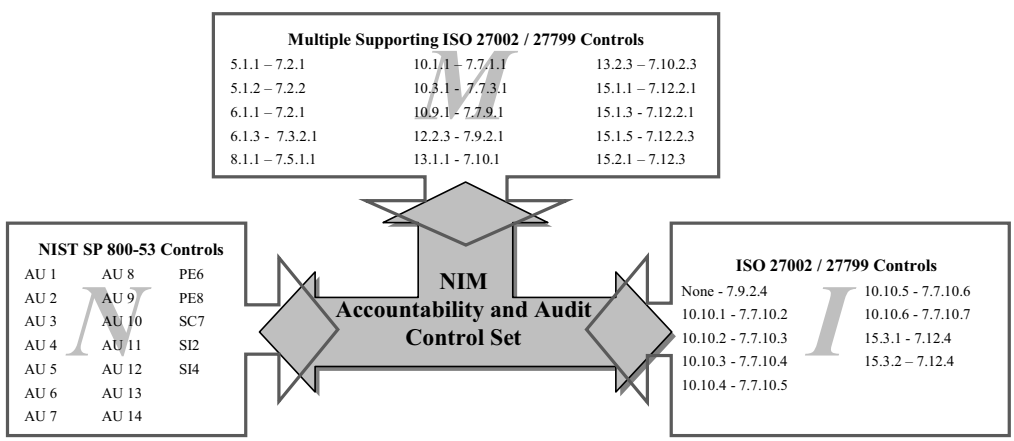

Figure 1 – NIM Accountability control set

The focus shifted to the ISO 27002. The controls dedicated to accountability were identified. These are presented in Figure 1 as Arrow I which contains the ISO 27002 controls that are directly related to accountability. The SP 800-53 security control mapping was used again, this time to map the ISO controls to the NIST controls. This mapping rendered some NIST controls not contained in the AU family. The complete set of identified NIST controls are presented in Figure 1 as Arrow N.

The focus of this research is the healthcare industry, therefore, the ISO 27001 controls needed to be mapped to the ISO 27799 health specific standard. This was achieved using the work of [13] in which a mapping between the ISO 27002 and the ISO 27799 was done. It includes the extent of coverage offered to the security issues by each standard. It was observed that the ISO 27799 includes additional guidance to accommodate the unique needs of health information security.

The activities of accountability exist within a security program and its ISMS and are, as such, directly and indirectly related to other security controls. The mapping between the NIST and ISO 27002 identified ISO-controls that are indirectly related to accountability. These are included in the resultant control set as multiple supportive controls and are presented in Figure 1 as Arrow M. The mapping between the ISO 27002 and ISO 27799 is reflected in the diagram.

The completion of these steps rendered a resultant control set for Accountability. The Connecting for Health Common Framework was consulted, as an independent source, to provide an unrelated analysis of the completeness of the accountability and audit controls.

Results

The NIST AU-family of security controls cover the entire gamut of audit logging and mentoring activities and their related controls are inclusive of a variety of activities including risk management and access enforcement [10].

The ISO 27799 Monitoring security clauses contain additional guidance to satisfy the special, healthcare security requirements for audit and logging that will ensure accountability and provide an incentive to users to conform to a level of acceptable use [13]. It was apparent that due to the unique needs of healthcare accountability it was necessary to include the new ISO 27799 security control - 7.9.2.1. Uniquely identifying the subject of care - into the NIM Accountability control set. There are many references to the need for distinctive identification needs within the EHR and its PII. Healthcare accountability is strongly linked to the unique identification of the users, their actions and the subject (the patient) of their activities.

There are many references in the Audit Record Content to the identification of the user and patient to enforce the concept of accountability through traceability. This raises the importance of uniquely identifying the user and patient interacting with the HIS [14], [12], [10]. This reinforces the decision to include the ISO 27799 security clause 7.9.2.1 in NIM Accountability control set.

The inter-relatedness of the accountability controls is demonstrated in Figure 1. Arrow N presents the identified NIST controls, Arrow I presents the ISO-controls that are directly related to accountability and Arrow M presents the multiple ISO-controls that support accountability. The NIM Accountability control set is represented by the multi-directional arrow.

The NIM Accountability control set is presented in Table 1. It represents the control set at the union of the Arrows marked N, I and M. It tabulates, in full, the controls identified through the mapping between the NIST SP 800-53, the ISO 27002 and ISO 27799 and includes the additional healthcare specific control.

Table 1 – NIM Accountability control set

NIST	ISO 27002	ISO 27799
None	None	7.9.2.4
AU-1 AU policy & procedures	5.1.1, 5.1.2, 6.1.1, 6.1.3, 8.1.1, 10.1.1,10.10.2, 15.1.1, 15.2.1, 15.3.1	7.2.1, 7.2.2, 7.2.1, 7.3.2.1, 7.5.1.1, 7.7.1.1, 7.7.10.3, 7.12.2.1, 7.12.3, 7.12.4,
AU-2 Auditable events	10.10.1, 10.10.4,10.10.5, 15.3.1	7.7.10.2, 7.7.10.5, 7.7.10.6, 7.12.4
AU-3 Contents of audit records	10.3.1, 10.10.1	7.7.3.1, 7.7.10.2
AU-4 Audit storage capacity	10.3.1, 10.10.1	7.7.3.1, 7.7.10.2
AU-5 Response to audit failures	10.3.1, 10.10.1	7.7.3.1, 7.7.10.2
AU-6 Audit review, analysis & reporting	10.10.2, 10.10.5, 13.1.1, 15.1.5	7.7.10.3, 7.7.10.6, 7.10.1, 7.12.2.3
AU-7 Audit reduction & report generation	10.10.2	7.7.10..3
AU-8 Time stamps	10.10.1, 10.10.6,	7.7.10.2, 7.7.10.7
AU-9 Protection of audit information	10.10.3, 13.2.3, 15.1.3, 15.3.2	7.7.10.4, 7.10.2.3, 7.12.2.1, 7.12.4
AU-10 Non-repudiation	10.9.1, 12.2.3	7.7.9.1, 7.9.2.1
AU-11 Audit record retention	10.10.1, 10.10.2, 15.1.3	7.7.10.2, 7.7.10.3, 7.12.2.1
AU-12 Audit generation	10.10.1, 10.10.4, 10.10.5,	7.7.10.2, 7.7.10.5, 7.7.10.6
AU-13 Monitoring for information disclosure	None	None
AU-14 Session audit	None	None
PE-6 Monitoring physical access	10.10.2	7.7.10.3
PE-8 Access records	10.10.2, 15.2.1	7.7.10.3, 7.12.3
PL-6 Security-related activity planning	15.3.1	7.12.4
SC-7 Boundary protection	10.9.1, 10.10.2	7.7.9.1, 7.7.10.3
SI-2 Flaw remediation	10.10.5	7.7.10.6,
SI-4 Information system monitoring	10.10.2, 13.1.1	7.7.10.3, 7.10.1,

Discussion

There are a variety of defined and generally accepted concepts in the area of information security and information security management. It is pertinent to inspect some to frame the proposition that trust can arguably be controlled.

The goal of information security is seen as the "preservation of confidentiality, integrity and availability of information" and includes such terms as the accountability of users, authentication, non-repudiation and reliability [15]. The goal of health information security is stated as maintaining information confidentiality, availability and integrity including authenticity, accountability and auditability [14]. There is a subtle difference between the two definitions and the healthcare security requirements are more inclusive. Additional healthcare considerations include the compliance with data protection laws and privacy legislation, maintaining organisational and individual accountability and maintaining public trust in the healthcare provider and the HIS in use [14]. Notably, accountability, auditability and trust are central to the definition of security in the healthcare context.

The ISO 27799 Section 7.7.10 Monitoring covers audit logging and monitoring and states that "Of all security requirements protecting personal health information, among the most important are those relating to audit and logging. These ensure accountability for subjects of care entrusting their information to EHR systems and also provide a strong incentive to users of such systems to conform to the policies on the acceptable use of these systems…" [14].

There are frequent references in the security literature to the concepts of trust and accountability. These concepts are examined to clarify their relationship. Trust is defined as, according to [16], the firm belief or confidence in the integrity, reliability, honesty etc. of another person or thing. It has the following synonyms: assurance, confidence, certainty and belief.

Trust, as a concept in IT security, is seen as result of good information security. It is not explicitly defined and is seen as an intrinsic concept.

Accountability, conversely, is frequently defined in a variety of standards, practices and guidelines. Its main aim is to ensure that activities are attributable to individuals [12]; similarly as the "property that ensures that the actions of an entity may be uniquely traced to that entity" [14] or as "the security goal that generates the requirement for the actions of an entity to be uniquely traced to that entity." [17].

The question posed by this research is – can trust be controlled by the use of appropriate accountability measures? There is an imperative to maintain organisational and individual accountability and the public trust in the HIS. These, it is argued, can be seen as a function of the implemented security controls that promote the accountability of the users for the data [5].

An HIS environment often relies heavily on the trust of its users who act as "guardians'' to protect its information. Guardianship can be implemented through using IT in monitoring and auditing the system activities [3]. Monitoring and auditing activities are typically associated with the concept of accountability. Therefore, accountability may be improved, through the application of appropriate mechanisms, such as monitoring and auditing. An improvement in accountability may lead to an increase in trust. This is due to stakeholders being sure that all activities are uniquely attributable to individuals, who can be held accountable for their actions. Therefore, it can be concluded that there appears to exist a reciprocal relationship between the level of trust placed in an HIS and the degree of accountability of its users.

Self-regulation is a key element of trust. However, relying on the trust or ethics of the users, who enjoy a professional status, is in-adequate and some control measures are necessary. Strong, user-identification procedures strengthens the ability of the HIS to prove accountability through its audit processes. It is possible to uniquely trace all activities within the HIS through examining the audit records.

The NIM Accountability control set is proposed to cover all the aspects of accountability within a healthcare environment and is specifically expanded to strengthen the identification of the user and patient. It is necessary to examine how the NIM Accountability control set may strengthen accountability and, therefore, trust.

The ISO 27799 text underlines both the importance of and inter-relationship of accountability and trust. The implication is that the stronger the accountability measures, the greater the resulting trust because all system actions are uniquely traceable to an individual. The rationale is that these mechanisms ensure accountability for the patient who has entrusted his personal information to the HIS and that it is used in an acceptable manner [14].

An audit log and the traceability afforded by the EHR are an important benefit provided by the use of an HIS. Privacy and accountability can be ensured through the audit and logging mechanisms which record all the access, activities and use of the EHR [2]. Strong privacy protection is seen to enhance the quality of the data and the subsequent health care that can be provided, by increasing the trust and the amount of truthful information shared by the patients, according to [18]. The inclusion of transparent and effective logging and audit control practices will promote trust among both the patients and participating institutions [12].

Accountability is established when the activities of the users of the HIS can be uniquely identified through a meaningful audit trail which is created for the actions of the users who can be held responsible for their actions. It is argued that robust audit controls may produce a greater level of accountability through enhanced traceability which, in turn, may promote the level of trust in the HIS.

The NIM Accountability control set contains a set of robust audit controls which are augmented to satisfy the health-specific accountability needs of health information security. The NIM Accountability controls are designed to provide an increased degree of accountability, for an HIS, when implemented. The reciprocal relationship between trust and accountability implies that the level of trustworthiness of the HIS, as perceived by its stakeholders, can be improved by the use of the NIM Accountability control set.

The use of the NIM Accountability control set may promote a tangible culture of trust within the healthcare environment.

This may help overcome the barrier of treating information security as a serious threat issue [3].

There is link between strong audit mechanisms that promote accountability which may lead to a reciprocal increase in trust by the users and patients of an HIS. This is the rationale behind the argument that trust may be controlled by implementing strong accountability control measures which influence the amount of trust placed in an HIS by its stakeholders. An HIS which employs a set of strong audit controls, as provided by the NIM Accountability control set, may improve its accountability and therefore, its level of trust.

Conclusion

The increasing reliance of healthcare management on IT and use of the EHR has brought benefits which carry an increased but unrealised security risk. This security gap has affected the confidence of the stakeholders in the operation of an HIS. It has raised the issue of trust in the provision of healthcare IT services. The research argues that a reciprocal relationship exists between trust and accountability. The viability of implementing accountability controls or measures, in healthcare security, to strengthen trust is examined.

A literature based approach is used and the NIST SP 800-53, ISO 27002, ISO 27999 and Markle Foundation Connecting for Health Common Framework were examined. A set of augmented accountability controls, the NIM Accountability control set, were identified from these documents.

An area of future research is the creation of dedicated security performance measures which will measure the effectiveness of the NIM Accountability control set.

The NIM Accountability control set is inclusive of the special needs of an HIS. It is proposed that when the controls are implemented they create greater user accountability which may result in increased patient trust in the use of an HIS, therefore, trust may, arguably, be controlled.

Acknowledgements

The financial assistance of the National Research Foundation (NRF) is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily attributed to the National Research foundation.

References

[1] Williams P. A practical application of CMM to medical security capabilities 2008;16 (1): 58-73.

[2] Bakker A. The need to know the history of use of digital patient data, in particular the EHR. International Journal of Medical Informatics 2007;(76):438-441.

[3] Williams PA. In a 'trusting'environment, everyone is responsible for information security. Perth: Edith Cowan University;2008.

[4] Civelek A. Patient safety and privacy in the electronic health information era: Medical and beyond. Clinical Biochemistry 2009;(42):298-299.

[5] McCallister E, Grance T, and Scarfone, K. NIST Special Publication 800-122 (Draft) Guide to protecting the confidentiality of personally identifiable information (PII) 2009. Gaithersberg: National Institute of Standards and Technology;2009.

[6] McGraw D, Dempsey J, Harris L and Goldman, J. Privacy as an enabler, not an impediment: building trust into health information exchange. Health Affairs 2009;28 (2): 416-427.

[7] Williams PA. When trust defies common sense. Health Infomatics Journal 2008; 211-221.

[8] Barber B. Patient data and security: an overview. International Journal of Medical Informatics 1998;49:19-30.

[9] Alshawi S, Missi F, and Eldabi, T. Healthcare information management: the integration of patients'data. Logistics Information Management 2003;16 (3/4):286-295.

[10] Initiative Joint Task Force Transformation. NIST SP 800-53 Revision 3 Recommended security controls for federal information systems and organisations. Gaithersberg: National Institute of Standards and Technology; 2009

[11] Markle Foundation. Connecting for Health - The Common Framework 2006 [cited 2009 March]; Available from: URL: http://www.connectingforhealth.org

[12] Markle Foundation. (2006). Connecting for Health - The Common Framework - P7 - Auditing access to and use of a health information exchange 2006 [cited 2009 March]; Available from: URL: http://www.connectingforhealth.org

[13] Ngqondi T. Information security management standards and best practices: a healthcare perspective. 2009. Port Elizabeth: Nelson Mandela Metropolitan University.

[14] Technical Committee ISO/TC 215 Health Informatics. ISO/IEC 27799:Health informatics - information security management using ISO/IEC 27002. Geneva: International Standards Organisation; 2008.

[15] Joint Technical Committee JCT1. ISO/IEC 27002 Information technology- security techniques - Code of practice for information security management. Geneva: International Standards Organisation;2008.

[16] Webster's New World College Dictionary. (n.d.). trust [cited 2009 September]; Available from URL: http://www.yourdictionary.com/trust

[17] Stoneburner G, Goguen A and Feringa A. NIST SP 800-30 Risk management guide for information technology systems. Gaithersberg: National Institute of Standards and Technology; 2002.

[18] Markle Foundation. (2006). Connecting for Health - The Common Framework -T5 - Background issues on data quality 2006 [cited 2009 March]; Available from: URL: http://www.connectingforhealth.org

Address for correspondence

Mrs Debra Box
Debra.box2@nmmu.ac.co