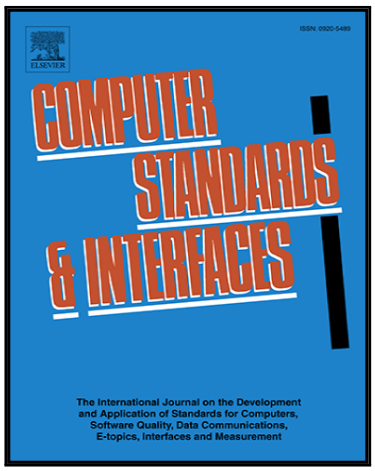

Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?

Scott Anderson , Professor Trish Williams

PII: S0920-5489(17)30231-3
DOI: 10.1016/j.csi.2017.10.001
Reference: CSI 3244

To appear in: *Computer Standards & Interfaces*

Received date: 16 June 2017
Revised date: 6 October 2017
Accepted date: 10 October 2017

Please cite this article as: Scott Anderson , Professor Trish Williams , Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?, *Computer Standards & Interfaces* (2017), doi: 10.1016/j.csi.2017.10.001

Highlights

- An analysis of technical guidance for cybersecurity of ISO 80001-2-8 is presented
- ISO 80001-2-8 technical security controls have significant gaps in areas
- ISO 80001-2-8 presents an effective baseline for cybersecurity of medical devices

Cybersecurity and Medical Devices: Are the ISO/IEC 80001-2-2 Technical Controls up to the Challenge?

AUTHORS

Primary & Corresponding Author:

- Scott Anderson, Flinders University, GPO Box 2100, Adelaide, SA, 5001. ande0548@flinders.edu.au

Co-Author:

- Professor Trish Williams, Flinders University, GPO Box 2100, Adelaide, SA, 5001. patricia.williams@flinders.edu.au

ABSTRACT

Medical devices, in the case of malfunction, can have tangible impact on patient safety. Their security, in a world where the Internet of Things has become a reality, is paramount to the continued safety of patients that are dependent upon these devices. The international standard ISO/IEC 80001 - *Application of risk management for IT-networks incorporating medical devices* presents a unified and amalgamated approach to the safety of medical devices connected to IT networks. Whilst this standard presents a guide for security and risk management in health delivery organisations, its effectiveness with regard to contemporary cybersecurity is unknown.

This research employed a structured review process to compare and analyse the ISO/IEC 80001 technical controls standards (ISO/IEC 80001-2-2 and ISO/IEC 80001-2-8), with contemporary cybersecurity best practice, guidelines and standards. The research deconstructed the technical controls and drew links between these standards and cybersecurity best practice to assess the level of harmonisation. Subsequently, a deeper analysis identified the areas of omission, coverage, addition or improvement that may impact the effectiveness of ISO/IEC 80001 to provide effective cybersecurity protection.

ISO/IEC 80001 aims to provide a minimal level of cybersecurity however this research demonstrates that there are deficiencies in the standard and identifies the important aspects of cybersecurity that could be improved. This situation has arisen due to the rapidly evolving nature of the cybersecurity environment and the protracted time to revise and republish international standards. This research identified several areas that require urgent consideration, including Emergency Access, Health Data De-Identification, Physical Locks on Devices, Data Backup, Disaster Recovery, Third-Party Components in Product Lifecycle Roadmap, Transmission Confidentiality, and Transmission Integrity. The research will provide health delivery organisations implementing ISO/IEC 80001, assurance as to the level of protection supplied by the ISO/IEC 80001 standard, and the areas that may need enhancement to increase cybersecurity protection and consequently increase in patient safety. Further, the outcomes are expected to influence development of the related international standard,

as the findings from this research are being provided to the International Organisations for Standardisation, TC215 Health Informatics, Joint Working Group 7, to inform the review of ISO/IEC 80001 currently in progress.

KEYWORDS

ISO 80001; Cybersecurity; Risk Management; Medical Devices;

FUNDING

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

1 INTRODUCTION

The international community has long recognised that introducing medical devices into hospital IT networks brings additional risks to the devices as well as the networks on which they operate (Grimes, 2011). ISO/IEC 80001 - *Application of risk management for IT-networks incorporating medical devices* presents a unified and amalgamated approach to the safety of medical devices connected to IT networks. This approach was created by unifying existing standards, and amalgamating these with risk management techniques and technical controls. As medical devices can have real impact on patient safety should they malfunction, their security in a world where the Internet of Things has become a reality, is paramount to the continued safety of patients that are dependent upon these devices (Eagles, 2008). This issue is compounded by the increasingly blurred line between software and hardware, resulting in increased complexity of managing such devices (Williams & McCauley, 2016).

Most medical devices contain embedded software, and devices range from implantable pacemakers and anaesthesiology monitoring equipment, to fitness accessories like the Fitbit. Given that many clinically-based devices may directly impact patient safety, the creation and subsequent implementation of a framework that sets specific values for acceptable levels of security is needed. Further, as many 'medical networks' are a standard corporate network with a multitude of medical devices attached to them, a piecemeal approach to addressing cybersecurity threats will leave exploitable gaps in any security measures (Fonash & Schneck, 2015).

ISO/IEC 80001 is a multipart standard for the protection of medical devices on networks using risk assessment techniques. It is comprised of two parts:

1. ISO/IEC 80001: *Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities* in10 sub-parts, dealing s with risk management techniques, guidelines and processes; and
2. ISO/IEC 80001: *Application of risk management for IT-networks incorporating medical devices -- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples* in 9 sub-parts dealing with technical controls and specifications to support the implementation of ISO/IEC 80001-1.

This sub-parts cover guidance for specific risk management aspects and strategies. The sub-parts that specifically relate to implementable security measures are:

- ISO/IEC 80001-2-8: *Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2,* which maps and translates the presented capabilities from ISO/IEC 80001–- *2-2: Guidance for the communication of medical device security needs, risks and controls* into implementable technical security controls.

ISO/IEC 80001-2-8 derives its controls from a 'what should be in place' perspective, and this provides an implementation guide for articulating the security capabilities from ISO/IEC 80001-2-2. The intended outcome of ISO/IEC 80001-2-8 is to provide a minimum required level of security for health delivery organisations. However, it does not assess the ability of the security controls to protect against cybersecurity incidents.

Figure 1 provides the context of the research in relation to existing parts of ISO/IEC 80001, based on and extrapolated from ISO/IEC 80001-2-2 and ISO/IEC 80001-2-8. What differentiates this research from ISO/IEC 80001-2-8 is the perspective taken to analyse the standards and best practice. This research takes ISO/IEC 80001-2-8 and analyses the suggested security controls from a cybersecurity perspective. In doing this, it identifies the omissions, gaps, and the strength of the standards suggested minimum level of security against contemporary cybersecurity best practice in an evolving threat environment.

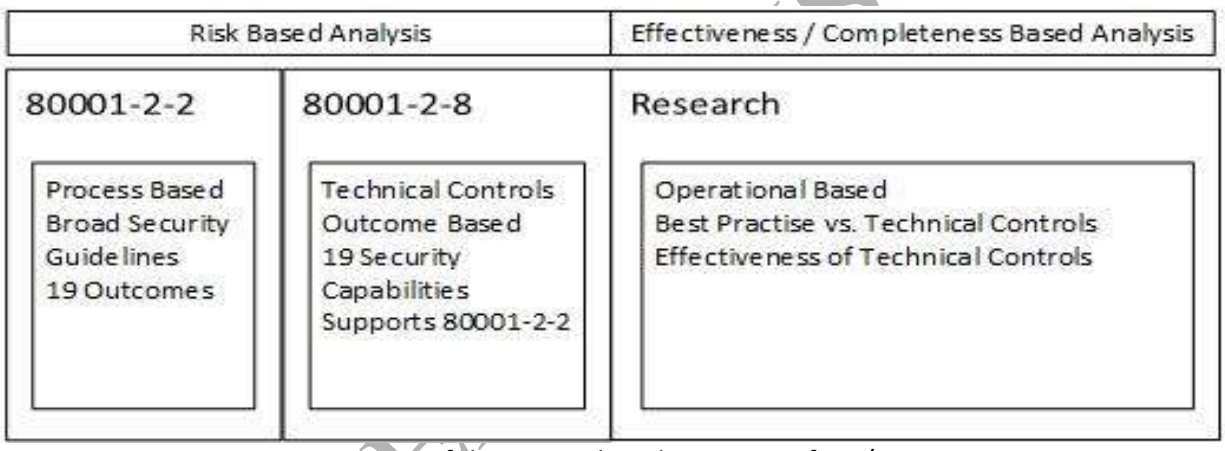

Figure 1 – Position of this research in the context of ISO/IEC 80001.

To date, there is no measure of the effectiveness of ISO/IEC 80001 implementations to provide protective assurance against cybersecurity incidents. This research contributes to addressing this issue.

1.1 BACKGROUND

There is an increase in the use of devices that are attached to medical IT networks, including medical devices and wireless mobile technologies (Cooper & Fuchs, 2013). While all medical devices require jurisdictional approval, for instance, the US has the Federal Drug Administrations (FDA) and Australia has the Therapeutic Goods Administration (TGA), they are rarely tested from a cybersecurity systematic perspective upon integration into a medical IT network. The international standard ISO/IEC 80001 is designed to assist organisations with the integration of medical devices into medical IT networks. The standard is risk based, and is segmented into 10 parts to address the broad areas of safety and effectiveness, together with data and system security. To facilitate this, the standard presents 19 security capabilities. These capabilities are outlined in ISO/IEC 80001-2-2 and listed in Table 1.

Capability Name	Acronym
Automatic Log-off	ALOF
Audit	AUDT
Authorization	AUTH
Configuration of Security Features	CNFS
Cybersecurity Product Upgrade	CSUP
Health Data De-Identification	DIDT
Data Backup and Recovery	DTBK
Emergency Access	EMRG
Health Data Integrity and Authenticity	IGAU
Malware Detection and Prevention	MLDP
Node Authentication	NAUT
Personal Authentication	PAUT
Physical Locks and Devices	PLOK
Third-Party Components in Product Lifecycle Roadmaps	RDMP
Software and Application Hardening	SAHD
Security Guidelines	SCUD
Health Data Storage and Confidentiality	STCF
Transmission Confidentiality	TXCF
Transmission Integrity	TCIG

Table 1 – List of Security Capabilities (ISO/IEC 80001-2-2)

Complementing this is implementation guidance in ISO/IEC 80001-2-8, which includes specific actions to take and expected results. ISO/IEC 80001-2-2 and ISO/IEC 80001-2-8 detail how to assess risks associated with medical device usage and implement controls balanced across the 19 security capabilities.

1.2 Problem

The effectiveness of the 19 security capabilities in ISO/IEC 80001-2-2, and the technical guidance in ISO/IEC 80001-2-8 to provide practical cybersecurity protection, is unknown. As such, an analysis of the technical controls and guidance provided by ISO/IEC 80001-2-8 aligned with the 19 security capabilities allows for the identification of the areas of coverage, omission and improvement when viewing these controls with a cybersecurity outlook. The logical question of "how secure is the medical device" (Mankovich & Fitzgerald, 2011) is not one that the ISO/IEC 80001 standard seeks to answer, instead it looks to manage the risk associated with the usage of that device. This paper analyses the guidance provided by ISO/IEC 80001-2-2 and 2-8, in order to ascertain the level of completeness with regards to contemporary cybersecurity best practice.

2 Methodology

The following section details the theory supporting the research and the research design.

2.1 Methodology Selection

This research used information systems theory (Figure 2) to understand the interplay between different information systems, security standards, industry based practical guidelines, implementation factors, and theoretical framework.

As the research is concerned with medical IT networks and the effectiveness of the ISO/IEC 80001 series in minimising risk from cybersecurity incidents, the research needed to examine the information system components comprising of interaction between the human (processes), the technical aspects and the environment of context.

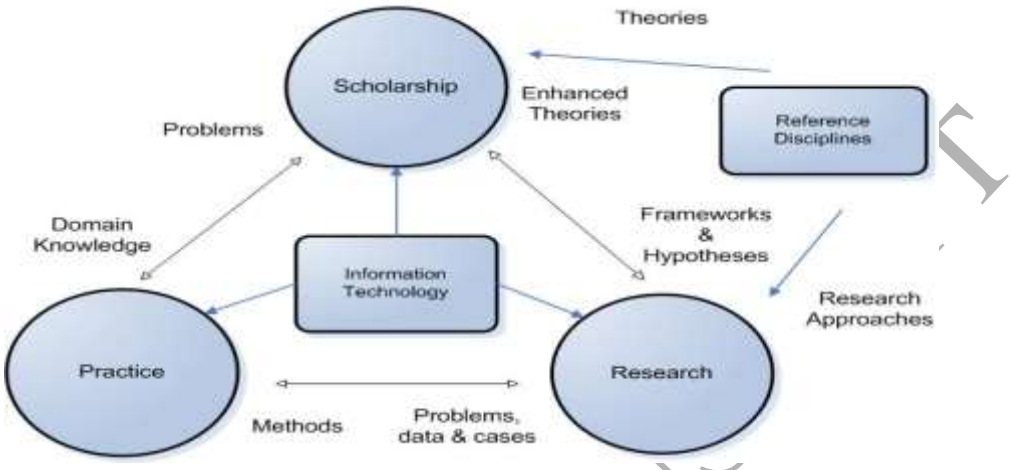

Figure 2. A Model of the Discipline of Information Systems (Shanks et al, 1993)

Exploratory research is the systematic usage of knowledge to generate new knowledge (Nunamaker & Chen, 1990). This research was both exploratory and applied, as the analysis of the effectiveness of the ISO/IEC 80001 cybersecurity controls takes the interpretations generated to extend the existing knowledge base. This was undertaken by answering the following questions:

1.) To what extent does ISO/IEC 80001 support contemporary best practice in cybersecurity protection?
2.) What recommendations can be made for improved protection from cybersecurity incidents using ISO/IEC 80001?

The approach employed a structured review of the existing standards, with specific focus on practical implementations and cybersecurity operations. This review analysed the existing standards by deconstructing them into constituent parts, then analysing the controls presented in each of the 19 security capabilities in order to ascertain correlations, coverage, omissions, gaps and improvement. This approach was selected as each standard is both an individual document and part of a larger whole. When examining the ISO/IEC 80001 standard it is important to understand how each individual segment of the standard fits into an overall system to be able to draw comprehensive practical conclusions.

Figure 3 illustrates the research design. The research was constructed in two distinct phases, cybersecurity framework analysis (Phase 1) and ISO/IEC 80001 analysis (Phase 2). Phase 1 was further sub divided into two concurrent activities: an analysis of cybersecurity frameworks, and an analysis of ISO/IEC 80001-2-2 and 2-8. The cybersecurity framework analysis identified common principles across the selected cybersecurity, best practice and standards documents.

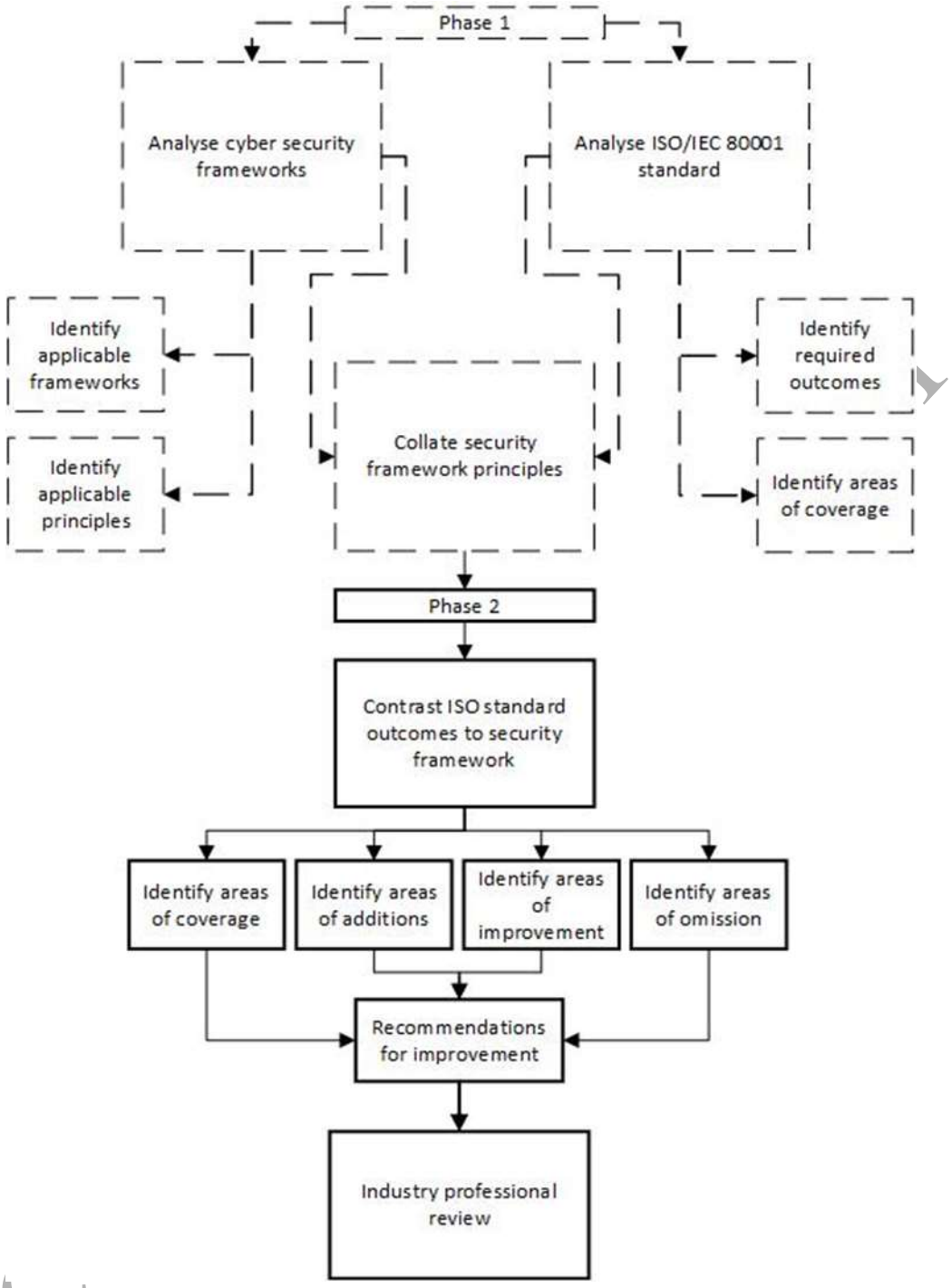

Figure 3. Research design

2.2 PHASE 1: ANALYSE CYBERSECURITY FRAMEWORKS.

Phase 1 analysed the contemporary cybersecurity standards and guidelines to compile a list of techniques, guidelines and practices. The National Institute of Standards and Technology (NIST) SP 800-53 document was selected as a common and mandated standard for federal usage in the US, and has also seen adaptation and adoption around the world. This document is risk-based, allowing for more direct correlation between this standard and the ISO/IEC 80001 prescribed controls. This was supplemented with the *Penetration Testing Execution Standard Technical Guidelines (PTES, 2012),* which was selected for the comprehensive and detailed information it provides. Further, the *Penetration Testing Framework 0.59 (PTF)* (Orrey, n.d.) was selected for correlation purposes. Both

these guidelines lead industry best practice for performing penetration testing, and thus allow for an external viewpoint for correlation. Such correlation is important as a baseline for cybersecurity best practice, as well as a measure of the strength of the controls under examination. Lastly, to ensure complete cross referencing with other ISO standards used in the development of ISO/IEC 80001, the following standards are also used as they were specifically referenced in ISO/IEC 80001-2-8:

- ISO/IEC 15408-2 *Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security Functional Components* (ISO/IEC 15408-2).
- ISO/IEC 15408-3 *Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Components* (ISO/IEC 15408-3).
- IEC 62443-3-3 *Industrial communication networks- Networks and System security – Part 3-3: System security requirements and security levels* (IEC 62443-3-3).
- ISO 27002). *Information technology - Security Techniques – Code of practice for information security controls* (ISO 27002).
- ISO 27799 *Health informatics – information security managements in health using ISO/IEC* 27002 (ISO 27799)

2.2.1 Phase 1: Analyse ISO/IEC 80001 standard.

An analysis of each of the 19 security capabilities (ISO/IEC 80001-2-2) was undertaken to look for harmonisation between the technical controls presented in ISO 80001-2-2 and 2-8. This also identified possible areas of omission, coverage, improvement and addition. Each of the 19 capabilities draws technical controls from five separate standards – SP 800-53, ISO/IEC 15408-3, IEC 62443-3-3, ISO/IEC 27002 and ISO 27799. This resulted in diagrams of varying complexity with the interlinking controls mapped and identified. Figure 4 is the template used to generate the harmonisation mapping.

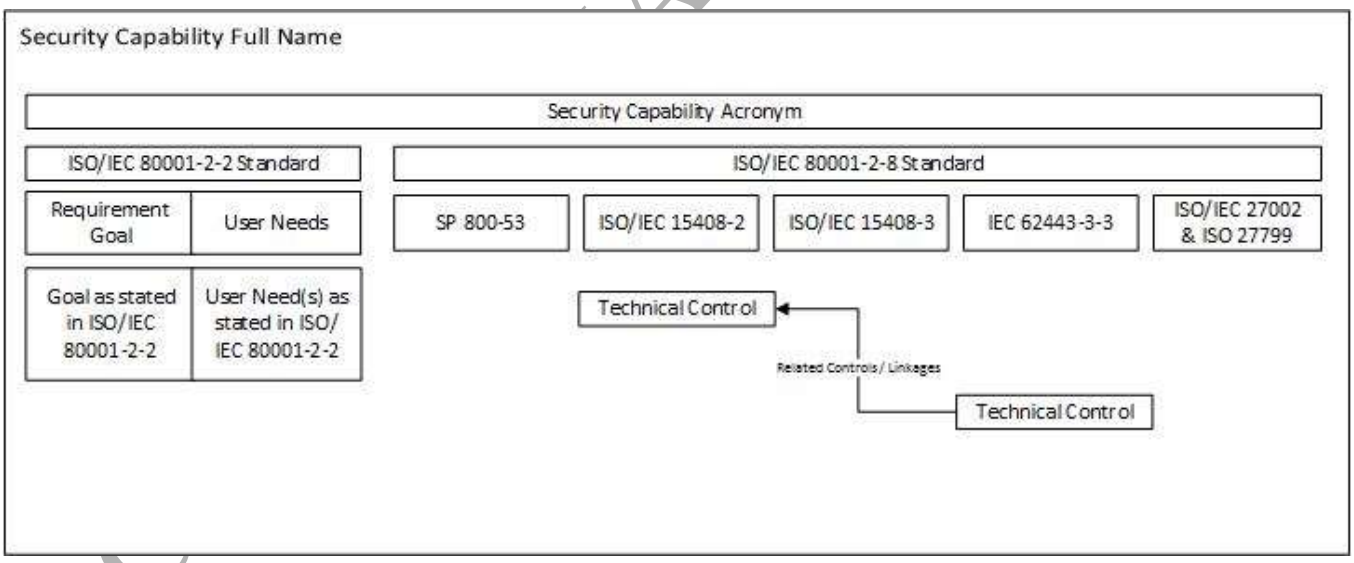

Figure 4. Harmonisation mapping template

The template in Figure 4 is used as follows:

1. The Security Capability Full Name and Acronym are directly linked to the 19 security capabilities that are presented in ISO 80001-2-2.
2. The ISO 80001-2-2 Standard presents Requirement Goals and associated User Needs, which are presented under the ISO/IEC 80001-2-2 sub heading, and are analyzed for interlinkages.
3. The user needs are compared to the technical controls, as they are more finely grained than the Requirement Goals.

4. The ISO/IEC 80001-2-8 Standard pulls technical controls from multiple standards – each standard has its own column. These controls are marked with interlinkages, and are sometimes relatable directly to a user need.

2.2.2 Phase 1: Collate security framework principles.

To ascertain a baseline level of best practice for cybersecurity protection, the common outcomes, goals and techniques were collated from the selected documents (SP 800-53, PTES and PTF). This resulted in a baseline for which comparison and analysis could be made between prescribed technical controls present within ISO 80001-2-8 and contemporary cybersecurity best practice. This baseline was achieved by examination of the principles used in cybersecurity best practice and those that applied to medical device security.

2.3 Phase 2: Contrast ISO standard outcomes to cybersecurity frameworks

Phase 2 compares and contrasts ISO/IEC 80001-2-2 and 2-8 standard with the Phase 1 output. This comparison identified the areas of the standard that appear effective from a cybersecurity perspective, as well as those that could be improved with further explanation, or have gaps compared to the security framework and principles. Lastly, recommendations from the detailed analysis were devised and provided to the international standards community via the ISO Joint Working Group 7, for consideration in the current review and revision of the ISO/IEC 80001 series.

This comparison resulted in a set of tables synthesised from the analysis of identified principles and best practice with respect to the provided technical controls. This generated a mapping of technical controls to prescribed outcomes of the standards. The template of the analysis table that compared the extracted principles of these frameworks to the deconstruction of ISO/IEC 80001-2-2 and 2-8 is shown in Table 2.

Name	Analysis	Notes	Coverage Level
Security Capability Name (Acronym)	**Positive** Positive points from analysis of ISO 80001-2-2 and 2-8 **Improvement** Possible Areas of Improvement within the capability **Confusing Controls** Controls that do not appear to aid in the security capability **Justification** The justification for the observations	Analysis notes made by the researchers.	Overall coverage level as presented, and possible areas to address.

Table 2. Template for Analysis Table

3 Results

The results show each security capability in detail to identify the omissions and anomalies, and then provides a summary discussion based on the collation of these.

Figure 5 is an example of the diagrams created for each of the 19 capability controls. A full set of the deconstruction diagrams for the 19 security capabilities and associated analysis tables can be located at http://www.flinders.edu.au/digitalhealth/digitalhealth_resources.cfm.

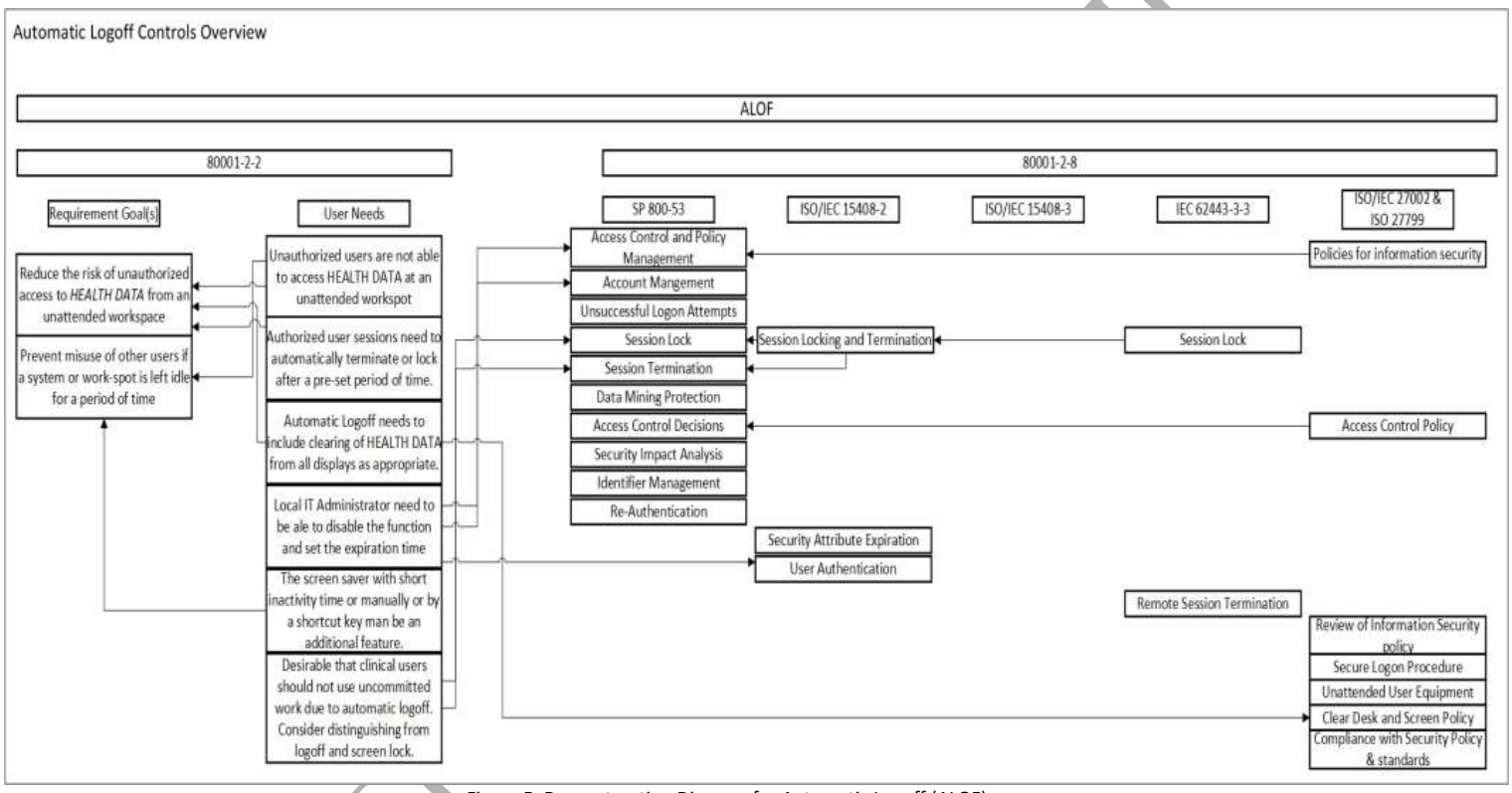

Figure 5. Deconstruction Diagram for Automatic Logoff (ALOF)

Figure 5 is one of the 19 deconstruction diagrams created from Phase 1 of the research process that created a baseline of best practice for cybersecurity protection, and identified common outcomes, goals and techniques.

Table 3 is one of the 19 analysis tables generated in Phase 2 of the research process. Using AUTH as the example, the table identifies the positive and improvable aspects of the technical control, together with extemporary notes and an assessment of the level of coverage the control provides from a contemporary cybersecurity perspective. A different example is used here, as the previous (ALOF) security capability does not present a sufficient coverage of the template.

Name	Analysis	Notes	Coverage Level
Authorization (AUTH)	**Positive** Local or Directory Based Maps to existing standards (X.509) Touches on *Least Access* and *Separation of Duties* Network segregation is also mentioned Documented Operating procedure **Improvement** Nothing about severity or scaled security controls as dependent upon *intended usage* **Confusing Controls** None **Justification** Security Principles: Authentication Authorization Least Access Separation of Duties	Relaxing controls when there is *"Adequate"* physical security controls in place creates a false correlation between physical security and the ability to relax authorization. What is the baseline for deeming physical security 'adequate'? Handling of assets Documented operating procedure could use a version or change control system.	Expansion on *"Adequate"* levels of physical security How assets should be handled Version or change control system for operating procedures

Table 3. Analysis Table for Authorization (AUTH)

3.1 CAPABILITY-CONTROLS FINDINGS

The results analysis table (as per the example in Table 3) provides the basis for the deductions and observations discussed below. This is reported by each of the 19 security capabilities, together with comment on the strength of the presented technical controls with respect to cybersecurity practical application, the issues identified with the capability, and the effectiveness in addressing practical cybersecurity protections.

3.1.1 Automatic Logoff - ALOF

The automatic logoff section draws from a well-established and robust area of cybersecurity. As such, there are minimal issues with this control. However, the need to tailor the advice given to account for 'real-life' usage is needed. In particular, the suggested screen timeout of 15-seconds to a minute is relatively short in elapsed time and could possibly impact the general usage of the device in a busy healthcare environment. Health delivery organisations would need to be aware of the intended usage for each type of user and tailor their policy on automatic logoff to reflect this. Overall, this control is effective and robust with respect to cybersecurity.

3.1.2 Audit - AUDT

There is room for clarification as to which controls are required for performing successful audit activities together with possible examples. However, the defined overall controls are effective.

3.1.3 Authorization - AUTH

Authorization draws from mature and established security protocols and therefore provides effective protection. There is omission of a change control procedure for authorization of people and systems integration.

3.1.4 Configuration of Security Features - CNFS

Configuration of security features is one of the largest areas covered by the standard, and covers extensive technical ground. This technical knowledge, along with the breadth and depth of required knowledge may create an issue for implementers without a comprehensive security background.

Additional guidance on principles and goals of the standard may help alleviate this potential lack of knowledge. The listed technical controls provide an effective baseline for configuration, dependent upon the implementer being able to utilise them effectively.

3.1.5 Cybersecurity Product Upgrades - CSUP

The configuration and management of cybersecurity upgrades is a common practice; however, the implementation nuances provide a substantial challenge. The logistical challenges of updating medical devices are unique to individual devices. The effectiveness of the standard may be improved by providing a baseline workflow example that allows for a health delivery organisation to construct or mimic the management of this process. With additional technical references and a higher level of harmonisation across standards, the effectiveness of this control can be increased without compromising the integrity of the standard. The reference to The OSI Guidelines for Security Vulnerability, Reporting and Response 2004 within the standard is contentious as the material is out of date by contemporary standards and practice in cybersecurity. This reference should be updated to a more recent standard that may consider revisions and discoveries that have occurred since publication. As international standards are designed to be platform agnostic, there is a conflict between the need for universally applicable guidance versus the technical information and guidance required to implement effective cybersecurity protections.

3.1.6 Health Data De-Identification - DIDT

Health Data De-Identification can be a problematic control as each health delivery organisation is required to conform to local legislative requirements. As such, the need for specific guidance is difficult to fulfil. The clarification of a reference stating pseudo-anonymization and its applicable use, while not directly affecting effectiveness, would create less confusion on why the standard is listed. This could be further improved by creating a workflow example as to how this de-identification should proceed, as well as referencing additional applicable technical standards that may help clarify the salient points. As the onus lies with the health delivery organisation and local regulations, this control is theoretically effective but difficult to implement.

3.1.7 Data Backup and Disaster Recovery - DTBK

Disaster Backup and Recovery is similar to Authentication, as a well-known and practiced cornerstone of cybersecurity, as well as a general good security practice. However, this control suffers from a lack of depth in the technical controls provided. There is a lack of advanced backup methods suggested as part of the technical controls. For example, there is no consideration and direction on the usage of criticality ranking to determine backup frequency, tiered backup systems and ‘hot’ or ‘cold’ sites. The addition of dedicated disaster recovery and backup standards would help alleviate this, as well as provide a more effective listing of controls and guidance. Clarification is also required for the definition of a ‘low powered’ device. As these devices are specifically mentioned, additional definition of the characteristics and guidelines that defines such a device is

preferable. This would also include the definition of the 'timeframe' stated within the standard for data retrieval from such devices, as this timeframe has neither explanation nor contextual advice. The listed technical controls are adequate and provide some measure of protection, however the area would benefit from more detailed guidance.

3.1.8 Emergency Access - EMRG

Emergency Access or 'Break -Glass', from a cybersecurity perspective, is a major vulnerability in any security system. The 'default', or commonly used pre-staged accounts, complete with easy to remember passwords and usernames, goes against basic cybersecurity principles. That these accounts usually compromise system or root level accounts, also exacerbates this risk. Whilst some mitigation guidance is provided in the form of additional physical security to prevent misuse, the utilisation of additional auditing controls, and dedicated clean-up upon usage of these accounts, this does not aid in hardening the vulnerability that providing emergency access creates.

The inclusion of the *Break-Glass – An Approach to Granting Emergency Access to Healthcare Systems* (Brucker & Petritsch, 2009) whitepaper on reactive break-glass access would provide an alternative method, utilising reactive group policy for access without the need for pre-staged accounts. The use of this type of system would alleviate some of the security flaws that are present with of pre-staged accounts. Ultimately, either system allows for an effective system for emergency access.

3.1.9 Health Data Integrity and Authenticity - IGAU

Maintaining the authenticity and integrity of health data is a multifaceted issue. It requires proper authorisation and data control measures, and relies upon the health delivery organisation's interpretation of the applicable legislation. As such, the control is effective in the sense that it provides a basic frame of reference. However, it is still left to the health delivery organisation to identify the relevant controls as per their legal requirements.

3.1.10 Malware Detection and Protection - MLDP

The control provides an effective baseline for cybersecurity because of the mature nature of existing practice in this area. As malware protection and detection is a key aspect of cybersecurity, the technical controls provided are well defined. Clarification on the use of the term 'safety' is needed, as it does not specify if this relates to 'patient safety' or 'cybersecurity safety'. It should be noted though that the need for high level technical knowledge in this control may lead to unintentional gaps in security. The addition of technical references or workflows that demonstrate a basic process, would allow for health delivery organisations to have a baseline that can then be customized to their needs.

3.1.11 Node Authentication - NAUT

To effectively analyse the connections between the controls, and make appropriate decisions on control requirements, it was necessary to further segment NAUT into:

- Users and Accounts
- Policy
- Management and Administration
- Auditing and Cryptography

As the technical controls provided are extensive, identification of what they cover and their intended purpose of use was difficult to identify. Whilst the overall control is comprised of a core set of controls aimed at governance and application, there are minimal specific controls that can be

accredited to Node Authentication as a process. This aside, the section benefits from the maturity of the authentication process.

3.1.12 Personal Authentication - PAUT

Given that this control is almost identical to NAUT, the question as to whether this is a needed control is raised. The clarity and effectiveness may be enhanced by combining the two controls into Authentication, with Node and User controls listed as a sub-set.

3.1.13 Physical Locks on Devices - PLOK

The physical security controls suffer from a lack of specific guidance in implementation and makes a fundamentally flawed assumption that increased physical security leads to a decrease in the need for Authentication (AUTH). Whilst the technical controls listed supply 'ideal' outcomes, the omission of implementation specifics, such as the technologies to be used and suitable physical access methods, weakens the effectiveness of this area. Overall the controls presented allow for an effective baseline of physical security, however improvements can be made by clarifying the 'what' and 'how' of the controls. Whilst this is at odds with a platform agnostic standard, the addition of dedicated physical security references would allow for this clarification whilst preserving the universal application of the standard.

3.1.14 Third-Party Components in Product Lifecycle Roadmap - RDMP

The management of third-party devices and software components presents a significant logistical challenge. Within complex networks the stated goals are quite broad, and whilst the technical controls are geared towards a process being created to manage the multitude of devices, there is nothing on which to base this process. The inclusion of an example workflow that covers a basic lifecycle would provide a solid starting point which the health delivery organisation could tailor towards their specific needs. This would further enhance this already effective control, leading to greater overall security.

3.1.15 Software and Application Hardening - SAHD

Software and application hardening is one of the broadest areas that cybersecurity is applied to, and as such requires extensive knowledge and time to apply effectively. While there is specific mention of medical devices and maintaining intended usage, there is no differentiation between the different types of software and hardware that may be present on a medical IT network. The prescribed controls present an effective base level of security. The reliance upon the SP 800-53 standard can be identified as a weakness as an overreliance upon a single document. The result is still an effective listing of controls, as SP 800-53 is highly specialized.

Additional information on more complicated aspects of SAHD would benefit the controls. For example, references to systematic testing guidelines. As with the MLDP control, the level of technical knowledge and expertise required to implement the controls is significant, and not every implementer will have these skills. Even without additional clarification, this section is still effective at providing a baseline of cybersecurity protection.

3.1.16 Security Guidelines - SGUD

These guidelines cover the basic principles of security that are applied in all aspects of cybersecurity, such as Least Access and Separation of Duties. This control also details the creation of clearly defined roles and responsibilities. These guidelines are applicable across all aspects of the standard, and present a solid foundation of security principles. This section also presents a challenge in terms of staff capability, as the requisite knowledge is highly specialised, causing the same issue as MLDP and SAHD, a possible lack of required knowledge.

3.1.17 Health Data Storage and Confidentiality - STCF

The security and confidentiality of health data at rest is highly dependent on the health delivery organisation's interpretation of the requirements of jurisdictional regulations. Whilst there are some technical controls listed, this area relies almost entirely upon the ISO 27002 and ISO 27799 for technical controls. This area is theoretically effective, much like DIDT, however the implementation is difficult, as the health delivery organisation must abide by local legislation. This may cause confusion as the health delivery organisation will be required to spend resources to ascertain the pertinent regulations and apply the relevant controls.

3.1.18 Transmission Confidentiality - TXCF

The addition of transmission confidentiality is a limited control, and could possibly been seen as an afterthought. The technical controls listed lack specific guidance and control information and rely almost entirely on reference to local legislation. This is an omission with regards to effective direction in cybersecurity.

This raises the question as to why X.509 is specified. If a health delivery organisation implements X.509, this section of the standard becomes redundant. The specific mention of "Authenticated Nodes Only" should also be addressed. As written, this assumes that all health data transmission will be undertaken only by authenticated "Nodes". As a medical IT network is made up of a multitude of devices, both hardware and software, this is highly unlikely to be the case. As such, major clarification in the wording and intended scope of node authentication should be applied, as this section may lead to a confusing and unhelpful application of controls. The controls themselves benefit from the maturity of the subject, in similar fashion to AUTH. On their own, the controls provide an effective and robust control set, clarification of intended usage will allow for greater effectiveness.

3.1.19 Transmission Integrity - TXIG

The addition of transmission integrity suffers much the same as the TXCF capability, as it consists of a limited number of technical controls. Whilst the listed technical controls would be effective, the usefulness and necessity of this section can be called into question, as there is little foreseeable benefit of specifically implementing this section.

3.2 DISCUSSION

Overall, the articulation of the 19 security capabilities in ISO/IEC 80001-2-2 to the technical controls in ISO/IEC 80001-2-8 is effective at providing a minimal measure of cybersecurity, with some capabilities more robust than others. Whilst no completely ineffectual control areas were identified, there are significant areas for improvement. Table 4 summarises the extent of potential improvement required in relation to cybersecurity protection.

Effective Controls	Controls with Minor Improvements Possible	Controls with Major Improvement Required
AUTH, ALOF, MLDP	AUDT, CNFS, CSUP, IGAU, NAUT, PAUT, SAHD, SGUD, STFC	DIDT, DTBK, EMRG, PLOK, RDMP, TXCF, TXIG

Table 4– Summary of Controls Effectiveness

As shown in Table 4, AUTH, ALOF and MLDP are effective, as the maturity and refinement of security practices over a long period of time. As such, these capability areas are the most effective in the standard.

Those requiring minor improvements (AUDT, CNFS, CSUP, IGAU, NAUT, PAUT, SAHD, SGUD, and STFC) have clear areas of omission, improvement or addition that would provide a more robust level of cybersecurity when addressed. Overall these provide adequate protection against cybersecurity incidents.

The controls that require major improvement (DIDT, DTBK, EMRG, PLOK, RDMP, TXCF, TXIG), may have been later additions to the capabilities list and therefore less well developed. This is due to either a lack of content, misleading or confusing outcomes, lack of implementation guidance or ineffective controls.

A potentially more important consideration is the compound impact of multiple ineffective and incomplete cybersecurity controls in one system. As cybersecurity is applied to a system, a single weakness creates a compounding issue. Whilst this is most prevalent in cybersecurity incidents, there exists potential for this to impact patient safety.

A large section of the standard is left to health delivery organisation internal policy and adherence to the laws and regulations of their jurisdiction. In addition, the overall effectiveness of the standard remains dependent on the organisation for adherence and completeness of implementation. Without acknowledgement of this as a potential issue, organisations (particularly those without cybersecurity expertise) may be left unnecessarily vulnerable to cybersecurity incidents.

4 CONCLUSION

The research analysed and compared ISO/IEC 80001 technical guidance with contemporary cybersecurity best practice, with the aim of identifying the completeness of this technical guidance.

Initial review of the guidelines and standards in the sphere of cybersecurity related to medical devices on IT networks, provided the identification of the essential security principles concerning cybersecurity protection. This initial review formed the basis from which to draw comparisons between the technical controls in ISO/IEC 80001-2-8 and cybersecurity best practice. In critically analysing the controls, deconstruction of each control was necessary to assess its effectiveness in providing cybersecurity protective measures. This analysis and comparison included identification of controls that were effective, out of place, ambiguous or in need of improvement.

ISO/IEC 80001 currently allows for an effective baseline of security against potential cyber incidents. Whilst there are areas that need improvement, the current technical controls and guidance can be said to be 'adequate'. The issue of balancing the agnostic nature of an international standard with the in-depth technical information needed for effective cybersecurity protection is an issue for the ISO TC215 Joint Working Group 7 to review and ultimately for implementers to address.

One measure may be the creation of a framework that tests the implementation of the standard against the practical application of cybersecurity best practice. Such a framework would allow those responsible for the secure management of the network to identify the flaws before an incident, and subsequently contribute to the overarching goal of patient safety when using medical devices. This research lays the groundwork upon which to create such a framework.

The knowledge generated during this research was through the synthesis and analysis of existing frameworks and established cybersecurity practices. The research extends the work already done on ISO/IEC 80001-2-8 by providing a lens of cybersecurity protection rather than risk assessment. In doing this, a broader and more practical perspective on the protections described in ISO/IEC 80001 is provided together with recommendations for improving the standard.

From the perspective of research and scholarship, the contribution is to the International Standards Community, through Joint Working Group 7 (JWG7). This research contributes to the current redevelopment of the ISO/IEC 80001 series by providing areas that can be taken under consideration for action during the redevelopment process. In turn, by addressing the issues identified, this allows a greater level of credibility to the standard. This may indirectly lead to a greater adoption rate, as the standard is seen an effective measure to implement.

Indirectly, this research impacts the patients serviced by a health delivery organisation. Whilst the standard certification and implementation process itself is invisible to the patients, the result of increased cybersecurity helps to prevent a loss of confidence in their health delivery organisation's and their ability to provide effective care, by applying the risk reduction and mitigation factors that are present in ISO/IEC 80001. As the challenges that occur in the medical IT world are unique and evolving as cybersecurity threats evolve, a systematic and complete approach to using standards such as ISO/IEC80001 becomes imperative to provide effective protection of the technology as well as patient safety.

5 REFERENCES

Brucker, A. D., & Petritsch, H. (2009). Extending Access Control Models with Break-glass. In B. Carminati & J. Joshi (Eds.), *ACM symposium on access control models and technologies (SACMAT)* (pp. 197–206). New York, NY, USA: ACM Press. https://doi.org/10.1145/1542207.1542239

Cooper, T., & Fuchs, K. (2013). The Wireless Challenge: Technology Risk Assessment In Healthcare *Facilities. Biomedical Instrumentation & Technology, 47*(3), 202-207.

Eagles, S. (2008). An Introduction to IEC 80001: Aiming for Patient Safety in the Networked Healthcare Environment. *Biomedical Instrumentation & Technology*, 15-19.

Fonash, P., & Schneck, P. (2015). Cybersecurity: From months to milliseconds. *Computer*, *48*(1), 42–50.

Grimes, S. L. (2011). Using 80001 to Manage Medical Devices on the IT Network. *Biomedical Instrumentation & Technology, 45*, 23-26.

International Organization for Standardization. (2010). *ISO/IEC 80001 - Application of risk management for IT- networks incorporating medical devices -- Part 1: Roles, responsibilities and activities.* Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863

International Organization for Standardization. (2012b*). ISO/IEC 80001 - Application of risk management for IT- networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls.* Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57939

International Organization for Standardization. (2016). *ISO/IEC 80001 - Application of risk maanagement for IT-networks incorporating medical devices -- Part 2-8: Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2.* Retrieved from https://www.iso.org/standard/64635.html

Mankovich, N., & Fitzgerald, B. (2011). Managing Security Risks With 80001. *Biomedical Instrumentation & Technology, 45*, 27-32.

Nunamaker, J. F., Jr., & Chen, M. (1990). *Systems development in information systems research.* Paper presented at the System Sciences, 1990., Proceedings of the Twenty-Third Annual Hawaii International Conference on vol.iii, pp.631-640 vol.3, 2-5 Jan 1990.

Penetration Testing Execution Standard (2012). Penetration Testing Execution Standard Technical Guidelines. Retrieved from http://www.penteststandard.org/index.php/PTES_Technical_Guidelines

Shanks, G., Rouse, A. and Arnott, D. (1993) *A review of approaches to research and scholarship in Information Systems (Working paper series)*, Department of Information Systems, Faculty of Computing and Information Technology, Monash University, Australia.

Williams, P.A.H. and McCauley, V. (2016) *Always Connected: The Security Challenges of the Healthcare Internet of Things.* In the Proceedings of the IEEE World Forum on Internet of Things, IEEE. Reston VA Dec 2016, pp. 30-35.

6 VITAE

6.1 SCOTT ANDERSON

Scott Anderson is a PhD student with an interest in cybersecurity. Located at Flinders University in South Australia, he is a part of the Digital Health Research Centre. Especially interested in IoT, medical devices and their practical security concerns, his work aims to examine the impact cybersecurity has upon the intersection of IoT and medical devices.

6.2 PATRICIA WILLIAMS

Professor Trish Williams is Cisco Chair and Professor of Digital Health Systems at Flinders University in South Australia, and co-director of Flinders Digital Health Research Centre. Internationally recognised in her field, Trish applies 30 years' experience in healthcare computing to practical outcomes in cybersecurity, IoT, mobile health, medical devices, governance, and health software safety. A passionate contributor and advocate for digital health informatics standards, Trish is co-chair HL7 International Security Workgroup and nominated national expert on many ISO standards. Trish is the primary author of the Royal Australian College of General Practitioners -Computer and Information Security Standards.