Computer Standards & Interfaces 000 (2017) 1–10

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?

Scott Anderson*, Trish Williams

Flinders University, GPO Box 2100, Adelaide, SA, 5001, Australia

ARTICLE INFO

Keywords:
ISO 80001
Cybersecurity
Risk management
Medical devices

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.

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 [5]. 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 [3]. This issue is compounded by the increasingly blurred line between software and hardware, resulting in increased complexity of managing such devices [13].

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 [4].

* Corresponding author.
E-mail addresses: ande0548@flinders.edu.au (S. Anderson), patricia.williams@flinders.edu.au (T. Williams).

https://doi.org/10.1016/j.csi.2017.10.001
Received 16 June 2017; Received in revised form 6 October 2017; Accepted 10 October 2017
Available online xxx
0920-5489/

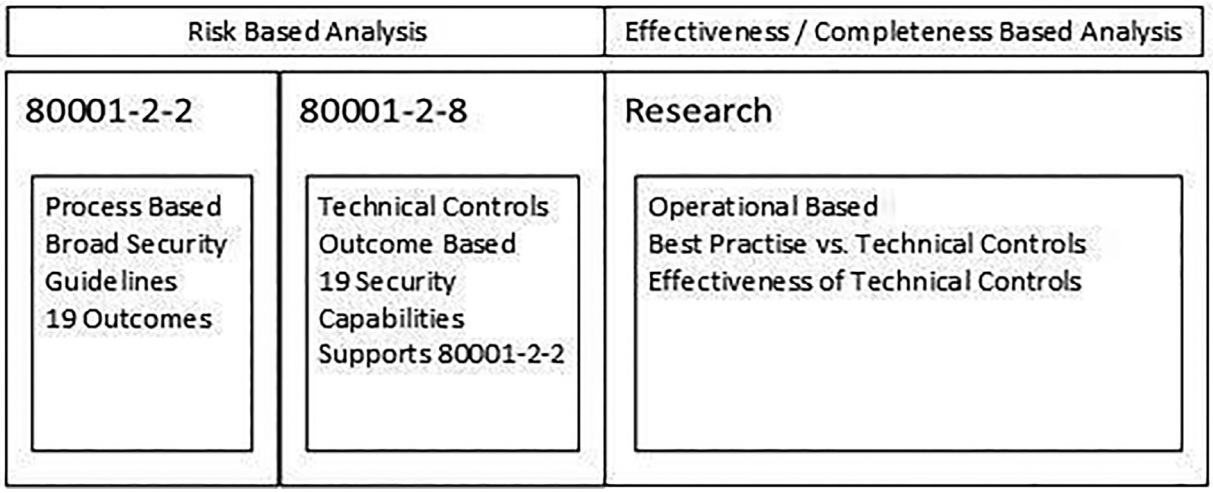

Fig. 1. Position of this research in the context of ISO/IEC 80001.

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 [6]: *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles*, responsibilities and activities in 10 sub-parts, dealing 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.

These 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 [7]: *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 [8]: *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.

Fig. 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.

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.

Table 1
List of security capabilities (ISO/IEC 80001-2-2).

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

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 [2]. 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.

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