Chapter 9
Hybrid Cyber Security Framework for the Internet of Medical Things

Danisa Nkomo and Raymond Brown

Abstract Despite IoMTs benefits in healthcare, emphasise that attaining robust security and privacy is becoming a huge challenge. The increased flow of information from IoMTs endpoints and applications increases the risk landscape; therefore, their security needs to be addressed. The risk to IoMTs includes potential harm to patient safety, compromise to patient health information and unauthorised access to devices. In 2013, 44% of data breaches occurred in the healthcare and in 2017, the National Health Service (NHS) England reported a ransomware attack which affected an estimated 80 trusts and an additional 603 primary care organisations. It is argued that for a sector (healthcare) under constant attack, the introduction IoMTs may be too big of a security risk. However, when the right security measures are in place, IoMTs can deliver more benefits than risk. With regards to The General Data Protection Regulation (GDPR), IoMTs raises compliance issues in the domain of consent. Cyber security frameworks such as ISO 27000 x series, NIST CSF 2018 or COBIT can be used as a guideline to implement security controls in IoMTs. However, some of them are out of date or lack the required approach to protect IoMTs technology. There is a lack of specific standards tailored to IoMTs security, and the need to safeguard patient safety, maintain the security and privacy of patient information that could all help towards more secure IoMT use cases. What is presented in this Chapter is a method to create a hybrid cyber security framework for IoMT. The framework is an extension of the NIST cyber security framework Version 1.1. This could be very useful to the UK healthcare industry as it is moving towards full adoption of IoMTs for benefits explained earlier.

Keywords Internet of medical things · IoT · BIG data · Blockchain · Privacy · Patient safety · IoMT endpoints · IoMT applications · Hybrid cyber security framework (HCSF) · NIST · Design science

D. Nkomo
Barnsley Local Authority, University of Northumbria, Newcastle upon Tyne, UK

R. Brown (✉)
Northumbria University London with QA Higher Education, Newcastle upon Tyne, UK
e-mail: Ray.brown@northumbria.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_9

9.1 Introduction

The Internet of medical things (IoMTs) or medical IoT are medical endpoints and applications with the ability to gather patient medical information and transmit to the desired remote visual platforms. The devices and software applications can self-connect to a gateway to transmit collected patient information (Alsubaei et al. 2017). The new technical ability of medical devices has led to more improved and efficient health care delivery, improved doctor-patient collaboration, adequate diagnosis and medical decision making. Whilst this is great for technological advancement and associated benefits, increasingly this involves the risk of security vulnerabilities.

Marr (2018) reported that the IoMTs endpoints and applications market is expected to reach a staggering 136.8 billion by 2021 worldwide and mentions that the number of medical devices connected to collect data and monitor patients will increase in the future. Marriott (2017) accepts that connected medical devices have considerable benefits in healthcare and the obvious advantages are; remote monitoring, automation, adaptability, precision medicine and local activity recording.

9.1.1 IoMTs Threat Landscape

IoMTs in healthcare present challenges in the privacy and security of information. According to FortiGuard cited in Adefala (2018), the most common threats are triggered by botnets which may take advantage of compromised IoT devices. Zhou et al. (2018) state that a compromised IoMTs device or application is more likely to initiate multiple attack vectors which may be hard to mitigate. Alsubaei et al. (2017) assert that IoMTs devices and applications increase the attack vector due to the complexity of the enabling technology (IoT). Most IoMTs are not secure by design; their wireless capability exposes them to the dangers of wireless sensor network security violations (Jadhav and Vatsala 2017). Most IoMTs solutions are operated, monitored and controlled by software applications. Therefore, there is risk coming from authentication and authorisation violations. Due to the issues mentioned above, the threat landscape for IoMTs has widened. These issues compromise the Confidentiality, Integrity and Availability (CIA) of critical patient data.

9.2 Attack Taxonomy

The need for intelligent patient monitoring and big patient data for effective decision making means the adoption of IoMTs will continue grow. It is expected that the threat landscape will also continue to increase. According to Ali and Awad (2018) different types of security threats can compromise the functionality of IoMTs networks. Some threats may be hard to predict, while other are obvious. The existing threats to IoMTs can be classified according to their attributes; network, information and host.

9.2.1 Information Based Attacks

Data in transit and data at rest can be intercepted by an adversary to remove information integrity (Chen et al. 2018). For an adversary to perform information-based attacks, the following methods are used:

- **Interception** – an attacker eavesdrops on medical information transmitted through the IoMTs network to compromise data privacy and confidentiality.
- **Modification** – an attacker gets unauthorised access to patient information, tampers with it to create confusion and deceive decision makers.
- **Fabrication** – false information is injected to threaten message authenticity as a result confuses decision makers such as doctors, surgeons, nurses or multidisciplinary teams.
- **Replay Attack** – can replay existing messages to threaten the message freshness.
- **Interruption** – an attacker instigates a distributed denial of service attack which breaks the IoMTs communication gateway. This type of attack threatens network functionality, device functionality, availability and is a risk to patient safety.

9.2.2 Host Based Attacks

These types of attacks are carried by taking advantage of host attributes;

- **User compromise:** an adversary compromises the users IoMTs device and network by obscurity or stealing. Such an attack is known to reveal sensitive information such as date of birth, social security, patient health data (Cafasso and Tarral 2018)
- **Hardware compromise**: an adversary tampers with the physical device where they can extract on device keys, data or programs. A tampered device can be reprogrammed or injected with malicious codes (Alharbi and Aspinall 2018).
- **Software compromise**: an attacker takes advantage of an out of date firmware, operating system of application to force to malfunction (Jadhav and Vatsala 2017).

9.2.3 Network Based Attacks

These types of attacks focus on the network layers and protocols protocol;

- **Standard protocol compromise**: an attacker compromises standard application and networking protocols and behave maliciously to threaten availability, integrity, privacy and authenticity.
- **Network Protocol Stack**: each layer of the protocol stack is vulnerable to attack. Therefore, an adversary may exploit this vulnerability by launching malicious activities (Gupta 2014).

9.3 IoMTs Privacy and Security Classification

The traditional architecture of IoMTs is composed of the perception layer, network layer and application layer, two more layers have been added; middleware and business layer (Ray 2016). The perception layer is composed of sensory devices. A sensory device detects and responds to some form of input from the physical environment. The most common inputs are heat, motion temperature, pressure or other things that can be sensed (Jadhav and Vatsala 2017). The output is a signal that is converted to human readable data. In most cases these will be transmitted over a network for further processing (Jadhav and Vatsala 2017). The Internet of Medical Things is classified into; wearable devices, implantable devices, ambient devices and stationary devices. Wearable devices enable continuous, real time and accurate monitoring of patients. The most common found in a modern healthcare set-up are pulse sensors, heart monitoring sensors, activity sensors, body temperature sensors, location sensors and glucose sensors. Other classifications are as follows:

Implantable devices – provide a visual of the body's internal systems such as a swallowable camera capsule or the embedded cardiac (Marriott 2017).

Ambient devices – these are used to monitor the patient's environment. Ambient devices are designed to monitor activity patterns such as the number of toilet visits, sleep quality or falls. Ambient sensors make the surrounding of the patient smarter. The most common ambient devices are motion, temperature, door, vibration, and pressure and daylight sensors (Marriott 2017).

Stationery devices – are devices isolated or not attached to the patient. These devices include imaging and surgical devices.

9.3.1 IoMTs Architecture and Attack Classification

The IoMTs defines a 3 layer architecture composed of the perception layer, network layer and the application layer.

The perception layer is the physical devices, which transfer the collected data to the network through a gateway. It is important to note that the perception layer is composed of physical devices which are wearable, implantable, ambient and stationery (Alsubaei et al. 2017). The perception layer as the lowest layer of the IoMTs architecture. Suo et al. (2012) also refers to the perception layer as the recognition layer. The role of the perception/recognition is to collect specified information from its surroundings; it collects parameters such as pulse rate, blood pressure, visual images, heartbeat and so on. The information collected is later digitised and transmitted to the healthcare network (HCSN) through a gateway.

The network layer is a data propagation platform; its main role is to facilitate content delivery to its specific destination. The network layer ensures the routing to the destination and network addressing is in check (Alsubaei et al. 2017). The network layer provides wired or wireless capabilities for IoMTs to be able to transmit the collected data. For example, magnetic resonance imaging requires high speed connection and reliable power source therefore require a wired medium (Alsubaei et al. 2017). Low powered IoMT devices may use wireless or radio technology to connect to each node or gateway. IoMT may also connect through to the IoT platform (Wireless Sensor Networks) which has Wi-Fi technology enabled (Anandarajan and Malik 2018).

The application layer is the highest level of IoMT architecture which consists of the middleware and business layer. This layer provide the information collected from the perception layers and displays them in various formats(Suo et al. 2012). The application layers provide the intelligence to make effective medical decisions.

9.4 Attack Classification and Mitigation

9.4.1 Perception Layer

Side Channel attacks: the attack method is based on the measurement of trends and frequencies of an IoMT device to ascertain a pattern. This can be used to extract private information from a system. In IoMT endpoints the transmission timing and power used probes can be used as an attack vector through the analysis of electromagnetic activity on the endpoints to extract patient sensitive data (Zhang et al. 2014; Yessad et al. 2017)

- **Tag cloning**: allows for the creation of a backdoor for data exfiltration from already established tags. The tag(cloned) may then be used to access patient data or a gain access to secure buildings (Ahson and Ilyas 2017).
- **Device tampering:** An IoMT endpoint's physical attributes can be compromised to alter its expected functionality therefore creating a potential risk to patient safety. For example, unsecure USB ports can be an entry point for malware injection (Yessad et al. 2017).

- **Sensor Tracking**: IoMTs endpoints have global positioning systems (GPS) to send patient location during an emergency; an attacker can spoof the GPS of an IoMTs and use this as an attack vector. Patient privacy is at risk from compromised sensors with fall detection capabilities (Yessad et al. 2017).

9.4.2 Network Layer

The network layer interfaces IoMT and the wider internet. Network technologies enables IoMT endpoints and applications communicate with other devices, applications and services in the internet (cloud) (Yessad et al. 2017). It is responsible for connecting IoMT endpoints and applications. Standard protocols define the rules and format that devices adopt to establish a connection. The IoT network is the underlying technology that enables IoMT and is composed of a 4 layer stack (Ahson and Ilyas 2017). The network layer in IoMT is susceptible to various attacks and the most common are;

- **Eavesdropping**: patient sensitive information can be captured during transmission and can be used as a path to launch a more evasive attack (Yessad et al. 2017). Encryption technology solves most of the eavesdropping attacks however it adds overheads which may affect the functionality of IoMT endpoints (Zhang et al. 2014).
- **Replay**: an attacker may recycle an authenticating message that has been exchanged before between authenticated users (Zhang et al. 2014). The authentication message would have been captured through eavesdropping. For example, replay attacks were highly effective in the One Touch Ping Insulin pump due to a vulnerable communication channel (Zhang et al. 2014).
- **Man-in-the-Middle**: a backdoor in IoMTs can allow an unauthorised user to replay legitimate authentication sequences to get access to the gateway (*Communication interface between IoMT and the healthcare network*) (Riahi Sfar et al. 2018).

9.5 The Importance of Cyber Security in IoMTs

From a cyber security perspective, the need for data security has become mandatory. Therefore, having the right security levels is essential to maintain the CIA of information. The application of good measure security controls builds confidence in the use of IoMTs and its use in healthcare improves patient quality of care and quality of experience. However, the exploitation of these devices through cyber hacking creates privacy and patient safety concerns. Marr (2018) states that cyber security in the healthcare industry helps to prevent patient information leakage and maintains patient safety. Therefore, any breach in this domain threatens patient privacy and exposes them to health risk. For example, a breach in a life critical IoMTs endpoint may compromise patient safety. Therefore, the security of IoMTs is critical to maintaining the privacy and safety of a patient.

9.5.1 Privacy

The lack of security by design of IoMTs creates vulnerabilities that can easily be exploited by an adversary (Ali and Awad 2018). IoMTs are the weakest link in healthcare information security chain. Therefore, insufficient controls may impact on patient privacy. An attacker using different attack techniques can penetrate the network and attack other IoMTs devices then control their operability (Zafari et al. 2016). A compromised, IoMTs device or software application can breach regulatory compliance such as the Data Protection Act (2016) and the General Data protection regulation (GDPR) 2016 which all attracts different fines under its provisions. Despite the general awareness of cyber security in healthcare, there has been a slow response to the constant emerging threat. It is essential to have security measures in mitigating against the ever-changing threat and to maintain the privacy of patient information.

9.5.2 Patient Safety

Patient safety is an essential aspect of the healthcare sector. The adoption of IoMTs in healthcare creates a huge concern for patient safety. Access to patient information may not be attractive to the attacker compared to the deadly cyber-attack on insulin infusion pumps attached to a patient in critical care (Yessad et al. 2017). This type of cyber breach may have a negative impact on the patient's life.

Chen et al. (2018) point out that malware leaks which are designed to steal personal information may impact on the IoMTs which create a risk to patient safety. Antonucci (2017) also points out that the reasons of prolific attacks in the healthcare sector are IoMTs lack robust security. Therefore, this leaves them more vulnerable to malware threats that probe them for such weakness. Many IoMTs devices such as the Continuous Glucose Monitors and insulin pumps run on the same operating system as consumer devices. Therefore, an automated hack cannot differentiate life-critical systems connected to the internet (Kurtz 2017).

A malware attack on a sensitive IoMTs device, such as glycaemic control device, may mean a patient could have severe consequences from an evasive device delivering hazardous drug loads to the patient (Kurtz 2017). There is overwhelming evidence that the threat to patient safety emanating from insecure IoMTs is real. In 2011 a study by Paul et al. (2011) reviewed the security of CGM and the insulin delivery system. The outcome of the study showed that an adversary could eavesdrop on the wireless communication and could control and alter the intended usage through impersonation. This potential harm to patient safety by vulnerabilities in IoMTs is a huge concern; it compromises the core principles of the healthcare sector. Any attack to IoMTs can have huge implications which are beyond malicious. For example, an attacker can wirelessly exploit vulnerabilities in pacemakers or make a deadly modification to insulin pumps of a large group of users, this may have a devastating impact on patient safety. Therefore, it is crucial to ensure adequate controls are put in place to maintain patient safety.

Following the privacy and security compromises to IoMTs, Zhou et al. (2017) stated that most cyber security risks can be prevented using existing frameworks, technology and standards. However, the dynamic nature of IoMTs creates new security challenges, and the key consideration is the accountability of risk which may not be aligned with today's threats landscape.

9.5.3 IoMTs Impact and Risk

Risk is the likelihood that a specified threat will take advantage of a weakness of an information asset (Jones and Ashenden 2005). Risk is measured as the likelihood of an event and the severity of an event (Katsikas 2013). Impact refers to the action of one object coming forcibly into contact with another (Jones and Ashenden 2005). In cybersecurity, the impact of a security breach is divided into economic cost, reputational damage and legal consequences (Ulsch 2014).

According to Biener et al. (2015), breaches often result in financial losses. Many people have entrusted the healthcare sector with their personal information, and any cyber breach compromises those trusting relationships (Biener et al. 2015). This could also damage the healthcare reputation and erode the trust held by patients. Data protection and privacy laws require organisations including healthcare to manage the security of personal data they hold. A security breach can comprise the personal data. Therefore, the organisation may face fines and regulatory sanctions under the new Data Protection Act of 2016 and GDPR (2016) provisions (Coventry and Branley 2018).

There is no doubt that IoMTs devices introduce risk, malicious actors may manipulate the flow of information from these devices or can tamper with the device. This may lead to a breach of valuable patient information resulting in loss of patient privacy and potential disruption to critical infrastructure. The implementation of security in IoMTs depends on its function within the healthcare organisation. What is more essential is to ensure the risk assessment is done following cyber security best practice, and that controls are in place to safeguard against the risk. The National Cyber Security Centre(NCSC) (2018a, b, c) points out that implementing security best practice is correlated to organisational risk. Therefore, this needs careful and robust attention.

9.6 Cyber Security Best Practice Frameworks

The best security practice should be strategic, operational and tactical. Following the past cyber security breach in healthcare. The best practice involves following the prescribed framework, standards and regulation that govern alignment with the healthcare sector. The best practices involve policies and procedures, frameworks and standards to identify any threats and vulnerabilities. These are then used to formulate incidence response methods along with recovery in case of disaster. In a healthcare environment the best practice assigned to cyber security are the following;

- ISO/IEC 27000: series is an international cyber security best standard and best practice (Van Haren 2014; International Standards Organisation 2018). It outlines how risk should be managed in information systems and provide controls for the security of information systems.
- ISO/IEC 27030: Internet of Things standards and best practice
- ISO/IEC 27799: offers guidance on security controls in healthcare and medical organisations (ISO 27001 Security 2018).
- NIST Cyber Security Framework Version 1.1: provides a framework for information security. It provides a policy framework of how an organisation can, identify, detect, protect, respond and recover from a cyber-attack (NIST 2018). CSF V1.1 now in incorporate the internet of things which is the enabling platform for IoMTs (NIST 2018).
- NIST Special Publication 800-53: a cyber security framework that incorporates the risk management framework to address cyber security controls for federal information (NIST 2018)
- Information Security forum: provide more thorough controls and direction on existing and evolving cyber security issues. it offers a comprehensive coverage of the provisions set out in the ISO/IEC 27002: 2013, COBIT 5 for information security, NIST CSF and the Payment Card Industry Data Security Standard (PCI DSS) version 3.1 (Information Security Forum 2016).
- HMG security policy framework (SPF) – a framework that provides principles to cover cyber security and these include; good governance, risk management, awareness, personal and physical security (NCSC 2018a, b, c).
- Health Information Trust Alliance (HISTRUST)- a framework that ensures information security in the healthcare sector. Through its common security framework, it ensures compliance with regulations and standards.

The above standards are focused on implementing the right security control, policies and procedures within an organisation. The best practice should be able to fit into the internal organisational processes. The complexity of the healthcare sector means the best practice adopts one framework combined with elements from other frameworks to ensure robust security.

9.6.1 Review of Cyber Security Best Practice Frameworks

The ISO/IEC 27000x series is a governance framework to manage cyber security in the organisation using policies and procedures at an operational level (International Standards Organisation 2018). The NIST SP 800-53 provides a practical way of implementing control through identification, protection, detecting, responding and recovering from an operational level. The Information Security Forum (ISF) is a process and business-driven, it provides a guideline for managing cyber security from a business perspective (NIST 2018). The ISF operates at a strategic and operational level within the organisation through the identification of gaps and setting goals to maturity levels (Information Security Forum 2016). Cyber essential is an entry-level assurance framework which provides guideline against the most common cyber threats on the internet and demonstrates that an organisation is committed to cyber security through implementation of the five technical controls (NCSC 2018a, b, c). HITRUST provide clear guidance to improve security using a risk-based approach to secure critical infrastructure and provide alternative controls.

9.6.2 IoMTs Best Practice and Principles

The cyber security best practice framework discussed above is not usable for IoMTs adoption. IoMTs adoption requires consideration of artefacts from various cyber security frameworks. It is important to note that there is no defined best practice in IoMTs. However, the best practice can be derived from the enabling technology (IoT) The best practice landscape within IoMTs are based on framework from other information systems. In IoT cybersecurity, consideration of frameworks tailored to other sectors is vital to secure IoT environment (Alsubaei et al. 2017). The Department of Homeland Security (2016) suggests that the best practice to manage risk and security of IoT enabled devices is adopting strategic principles. The best practice principles to security the IoT environment should;

- Ensure integration of cyber security in the design phase
- Advanced patch and vulnerability management
- Ensure cyber security measures are aligned with the potential impact of risk
- Promote transparency across IoT devices and infrastructure
- Perform proactive risk assessments and Identify whitelist applications
- Use of multi-factor authentication
- Create staff awareness and create incident response plans
- Regular data backup and limit administrative privileges

The IoT best practices support how cyber security is handled within an organisation. The adoption or introduction of new technologies such as IoMTs needs a new and different approach that is distinct from the generic cyber security framework and best practice. Alharbi and Aspinall (2018) state that the best practice can be used as requirements to design a framework and these should be based on the threat and vulnerability analysis. The requirements of IoMTs are risk specific, therefore, the best practice approach may fail to address cyber security in their complex environment.

9.6.3 Blockchain for IoMT Security

The adoption of IoMT provides the potential for big data analysis and effective medical decision making. However, the adoption of IoMT exposes the patient safety and privacy at risk. Therefore, there is an urgent need to find the most effective way to secure patient sensitive data. Also, failure to ensure the safety and privacy of patient information amounts to a breach of legislation and compliance. The security attributes offered by the blockchain technology have been considered to offer robust security of patient privacy. In addition, the technology (Blockchain) promises to reduce the risk of IoMT endpoints to be compromised through a central authority (Rivas and Wac 2018). Blockchain allows the creating of consensus groups on anomalous network behaviours and has the potential to fail-safe infected IoMT endpoints (Rivas and Wac 2018). Blockchain technology can quarantine any IoMT endpoints whose behaviour is questionable. However, the risk on this capability need to be clearly defined as it has the potential to impact on patient safety.

Blockchain embeds strong cryptography to each IoMT endpoint and creates a secure communication channel (Jesus et al. 2018). It is also ensures anonymity in IoMT use and guarantees patent privacy. Adopting the Blockchain technology offers effective traceability, patched management and maintains data security of IoMT (Trend Micro 2018). Other potential benefits includes the removal of single point of failure and building trust zones between IoMT processed (Trend Micro 2018).

9.6.4 IoMT and Big Data: The Impact of IoMT on Clinical Trials

In a clinical trial space, electronic record storage, data capture and digital trial management is the norm in most clinical research. IoMT as the enabler of Big data captures that data from patients from clinical trials. Using IoMT in clinical trials means behavioural change can be monitored effectively (Mishra et al. 2018). The IoMT capability of metric tracking allows the collection of accurate biological data from patients, which can then be shared between clinical research organisations (Iqbal 2017). Using data captured from IoMT along with accumulated clinical results creates more valuable clinical trials with ground-breaking results (Iqbal 2017).

IoMT capability to collect large volumes of data from patient creates the potential to make effective healthcare decisions(Ahmed et al. 2017). In healthcare, Big Data is mainly focused on machine or clinical data, transactional data and social data The Chartered Society of Physiotherapy (2018) state that big data is the future of healthcare delivery and data can be shared and analysed to improve patient safety and care. Big Data plays a big role in healthcare because of its potential to predict any outbreaks, improve quality of life and cure diseases. In a clinical setting, big data is used in evidence based practice to ensure patient safety.

9.6.5 Hybrid Cyber Security Framework (HCSF)

According to NIST (2018) a robust framework should focus on technology, processes and people.

Therefore, developing a cyber security framework must be based on several approaches for it to be effective.

A cyber security framework 's primary objective is to safeguard the CIA of IoMTs devices and applications. The framework incorporates guidelines from standards, regulatory compliance, best practice such as the ISO 27032, NISA CSF, Data Protection Act 2018 and GDPR 2018.

These features provide robustness in the security of IoMTs endpoints and software applications.

An effective cyber security framework requires the management of information security and is based on people, processes and technology. The HCSF pillars consist of IoMTs, Stakeholders, Technical and operational controls and Governance as illustrated in Fig. 9.1.

Consideration of this asset pillar involves the protection and mitigating critical IoMTs endpoints and applications. The protection should be done through the processes defined in the NIST CSF Version 1.1. IoMTs endpoints and software application are classified into; life critical, non-critical monitoring systems and wellness devices.

- ***Life critical IoMTs devices and applications*****:** These are safety critical medical endpoints and software applications. Any breach can have an adverse impact on patient safety. Therefore, their availability is critical. The security of life-critical systems and applications should be a top priority in an organisation. Assets in this category are; pacemakers, ventilators, defibrillator and insulin pumps.
- ***Non- critical monitoring devices and applications:*** Non- critical monitoring devices and applications record and transmit data in the same way as life critical systems, they do not monitor life-threatening conditions. Assets in this domain are glucose monitors. if a glucose monitor fails, the patient will require medical attention but not at the same level of urgency as a pacemaker or ventilator.
- ***Wellness devices*****:** Wellness devices and application track sleeping patterns, personal health and wellness such as fitbits or activity trackers. Wellness devices do not gather data to be relayed back to the healthcare professional.

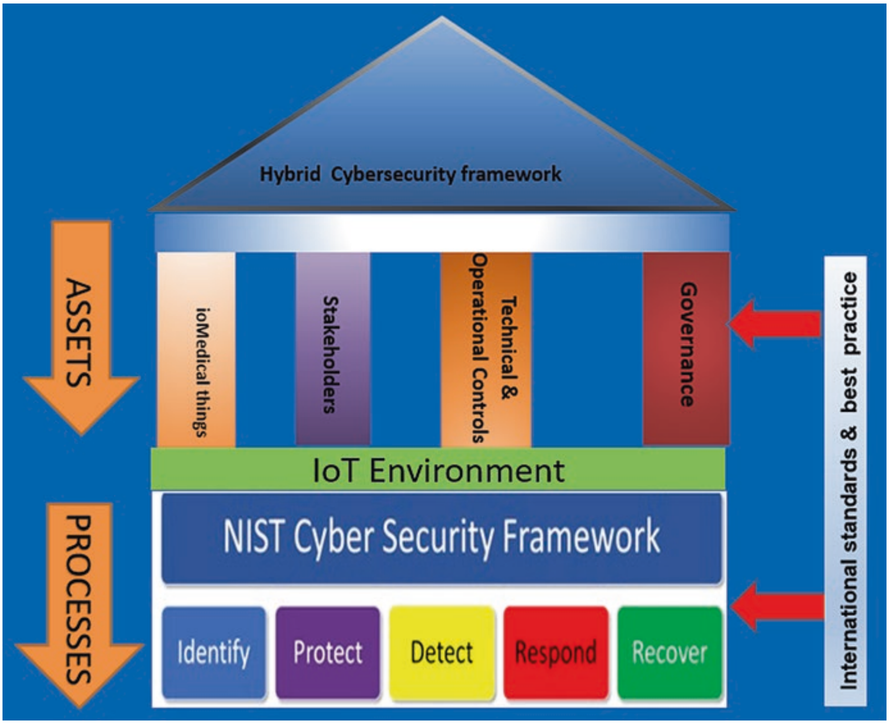

Hybrid Cybersecurity framework
ASSETS
ioMedical things
Stakeholders
Technical & Operational Controls
Governance
International standards & best practice
IoT Environment
PROCESSES
NIST Cyber Security Framework
Identify
Protect
Detect
Respond
Recover

Fig. 9.1 Assets and processes in IoMTs

According to Harbers et al. (2018), the development of a cyber security framework is challenged by a fractured process which mostly leads to more legislation to keep up to date with emerging threats. It is important to consider current legislation in a framework as it ensures compliance. The HCSF incorporate the Data Protection Act (2018), GDPR (2018), The Network and Information Systems Regulations 2018, the Health Insurance Portability and Accountability Act, PCI DSS. Also, it also incorporates the provisions of ISO 27030, 27779, Risk management in connected healthcare ISO 80001. Governance also involves best practice in the implementation of security controls.

9.6.6 Operational and Technical Controls

The operational and technical considerations include the security control measures to safeguard the CIA of critical infrastructure and assets pillars.

9.6.6.1 Stakeholders

These are people with a vested interest in and are affected by IoMTs. Such stakeholders include vendors, patients, clinicians, supplier, CISO, infrastructure teams and healthcare facilities. The CISO should be the primary stakeholder and driver of the HSCF. The internet service providers and power supply organisations will be among the key stakeholders.

9.6.6.2 Processes

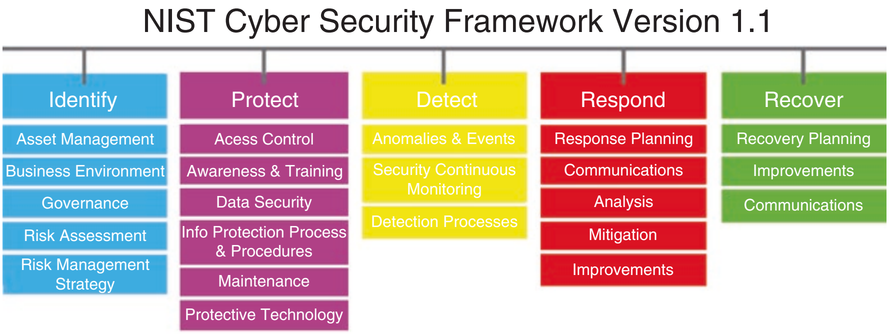
The HCSF is governed by processes to support its main pillars. These processes form the activities that occur within the pillars of the framework. The processes are taken from cyber security best practices such as NIST CSF Version 1.1 draft 2. The figure shows the processes from the NIST framework (Fig. 9.2).

- **Identify**

The identification of IoMTs assets and keeping an asset register is a practical approach towards maintaining the availability of services. The identification process in HCSF involve;

Asset Management IoMTs endpoints and application should be managed through an asset register. This should be done in line with their relative importance to the organisation risk strategy. The classification of endpoints and applications should be based on the value of maintaining patient safety, best practice and regulatory compliance.

Governance the policies, procedures and processes to manage and monitor regulatory, legal, risk, operational and environmental requirements are determined, and these should be part of the risk management.



NIST Cyber Security Framework Version 1.1

Identify	Protect	Detect	Respond	Recover
Asset Management	Acess Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Process & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Fig. 9.2 NIST Cyber Security Framework Version 1.1

Risk Assessment IoMTs endpoints and application threats and vulnerabilities are identified and documented following industry best practice. The potential impact and likelihood of a compromise to the IoMTs environment, endpoints and applications are identified.

Risk Management stakeholders should agree on risk assessment processes and how they should be managed. Risk tolerance should be established and clearly expressed.

- **Protect**

Access Control access to IoMTs environment, endpoints and application must be limited to authorised users or endpoints and applications limited to authorised activity. Identity and credentials should be managed for authorised endpoint and applications, and access permission should be granted on the principle of least privilege. For life-critical endpoints and application network integrity should be enforced through network segregation.

Awareness and Training users should be trained and informed of their roles and responsibilities within IoMTs. This also includes 3rd party stakeholders.

Data Security IoMTs data at rest and data in transit should be protected, and Integrity checking mechanism should be used to verify IoMTs software applications, firmware and information integrity. To ensure data security in IoMTs endpoints and applications, the production environment should be isolated from testing and development.

Protection Processes and Procedures IoMTs security policy should be integrated into a more comprehensive information security policy. The policy should address the scope, roles, coordination and management commitment. Protection policies must comply with current legislation and be improved on a regular basis. Response and recovery plans must be managed and tested in line with policies.

Protective Technology technical security solutions should be auditable and reviewed according to policies and procedures.

- **Detect**

Monitoring Monitoring at discrete intervals should be enforced to identify security compromises and to determine the effectiveness of protective measures. Monitoring for unauthorised personnel, connections, devices, and software should be performed.

Detection Processes roles and responsibilities should be defined to ensure accountability. Event detections reported to appropriate parties and that they comply with best practice. Detection processes should be tested on a regular basis to ensure applicability.

- **Respond**

Communication response activities should be coordinated with internal and external stakeholders. Where appropriate this should include support from law enforcement. Communication should be established in line with service level agreements and regulatory compliance. Information sharing should also ensure broader situational awareness.

Analysis this should be carried out to ascertain sufficient response and support recovery actions. This involves investigating notifications from IoMTs devices and applications. The impact of an incident should be understood, and forensics performed following cyber security best practice.

Mitigation activities should be carried out to prevent the spread of an event and mitigate its effect and get rid of the incident.

Improvement improvement should be developed from lessons learned from current and previous detection response activities.

- **Recovery**

Recovery Planning the recovery plan should be implemented during or after an event, and the recovery plan should integrate lessons learnt. The recovery strategy should be updated according to organisational policies and procedures.

Communication restoration of activities should be coordinated with internal and external stakeholders (Internet Service Providers, vendors, patients).

9.6.7 IoT Environment

The IoT environment is an enabling infrastructure for IoMTs endpoints and software application functionality. The IoT environment is interfaced with either the cloud environment or desired remote location. The IoT environment is composed of the gateway which manages the communication between IoMTs endpoints and the back-end systems. The IoT primary function is to route messages to and from endpoints (IoMTs devices and applications). Through the gateway, the environment can perform critical tasks such as device discovery, network driver deployment, management functionality, authentication and security set up. The IoT environment is a critical asset in this framework.

9.6.8 International Standards and Best Practice

International standards ensure the right policies and procedures are in place to comply with regulation and best practice. HCSF is supported by international standards in such ISO 2700 x series, HIPAA, ISO 80001 and the NIST CSF V1.1 draft 2. Also, HCSF is supported by cyber security best practice which creates a security culture within the organisation. The best practice in this domain means the stakeholders responsible for security should have a layered approach to security. In the case of medical IoT, they should have the ability to fail safe. In addition, best practice means following a risk-based approach to determine risk exposure and potential impact.

9.7 Conclusions

The key assets of a hybrid Cyber Security framework are IoMTs endpoints, software applications, stakeholders, technical and operational controls and governance. The processes are used to support the efficiency of control assets with requirements based on regulatory compliance. The application of Design Science Research informs the development and attempts to stretch the boundaries of human and organisational ability by creating new and ground-breaking artefacts such as methods, constructs, models and instantiations (Hevner and Chatterjee 2010).

The proposed hybrid cyber security from IoMT is adopted from the NIST Version V1.1. The framework is supported by security best practice and international standards. A layer of the IoT environment sits between the framework processes and the asset pillars. This is a gateway to the corporate network. Although, the lack of relevant cyber security framework in the UK in this domain meant benchmarking is restricted, however, an attempt to benchmark was made to determine how the framework performs against well-established cyber security framework. The prototype hybrid security framework is specific to medical IoT and is based on the NIST framework making it more robust in the provision of cyber security control medical IoT.

References

Adefala L (2018) Healthcare experiences twice the number of cyber attacks as other industries. Retrieved from https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

Ahmed E, Yaqoob I, Hashem I, Khan I, Ahmed A, Imran M, Vasilakos A (2017) The role of big data analytics in internet of things. Comput Netw 129:459–471. https://doi.org/10.1016/j.comnet.2017.06.013

Ahson S, Ilyas M (2017) RFID handbook. CRC Press

Alharbi R, Aspinall D (2018) An IoT analysis framework: an investigation of IoT smart cameras' vulnerabilities. Living in the internet of things: cybersecurity of the Iot – 2018. https://doi.org/10.1049/cp.2018.0047

Ali B, Awad A (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 18(3):817. https://doi.org/10.3390/s18030817

Alsubaei F, Abuhussein A, Shiva S (2017) Security and privacy in the internet of medical things: taxonomy and risk assessment. 2017 IEEE 42Nd conference on local computer networks workshops (LCN Workshops). https://doi.org/10.1109/lcn.workshops.2017.72

Anandarajan M, Malik S (2018) Protecting the Internet of medical things: a situational crime-prevention approach. Cogent Med 5(1):1–23. https://doi.org/10.1080/2331205x.2018.1513349

Antonucci D (2017) The cyber risk handbook, 1st edn. Wiley

Biener C, Eling M, Wirfs J (2015) Insurability of cyber risk: an empirical analysis. SSRN Electron J. https://doi.org/10.2139/ssrn.2577286

Cafasso M, Tarral M (2018) Designing flexible sandboxing solutions to adapt to new malware trends. Comput Fraud Secur 2018(2):5–9. https://doi.org/10.1016/s1361-3723(18)30013-7

Chen K, Zhang S, Li Z, Zhang Y, Deng Q, Ray S, Jin Y (2018) Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J Hardw Sys Secur 2(2):97–110. https://doi.org/10.1007/s41635-017-0029-7

Coventry L, Branley D (2018) Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 113:48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Department of Homeland Security (2016) Strategic principles for securing the internet of things (IoT). Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Gupta M (2014) Handbook of research on emerging developments in data privacy advances in information security, privacy, and ethics (1st edn.). IGI Global

Harbers M, Bargh M, Pool R, Van Berkel J, Van den Braak S, Choenni S (2018) A conceptual framework for addressing IoT threats: challenges in meeting challenges. In: Proceedings of the 51St Hawaii international conference on system sciences. https://doi.org/10.24251/hicss.2018.278

Hevner A, Chatterjee S (2010) Design research in information systems. Springer, New York

Information Security Forum (2016) The standard of good practice for information security 2016. Retrieved from https://www.securityforum.org/uploads/2016/07/SoGP-2016-Exec-Summary-FINAL-260716.pdf

International Standards Organisation (2018) ISO/IEC 27030 — Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT) [DRAFT. Retrieved from http://www.iso27001security.com/html/27030.html

Iqbal S (2017) IoMT and big data: the impact of the Internet of medical things on clinical trials. Retrieved from https://knect365.com/clinical-trials-innovation/article/5024ec64-030e-4ba6-bc2b-c701a28b2b95/big-data-and-iomt-the-impact-of-the-internet-of-medical-things-on-clinical-trials

Jadhav R, Vatsala V (2017) Security issues and solutions in wireless sensor networks. Int J Comput Appl 162(2):14–19. https://doi.org/10.5120/ijca2017913256

Jesus, E., Chicarino, V., de Albuquerque, C., & Rocha, A. (2018). A survey of how to use blockchain to secure internet of things and the Stalker attack. Secur Commun Netw, 2018, 1–27. doi: https://doi.org/10.1155/2018/9675050

Jones A, Ashenden D (2005) Risk management for computer security. Elsevier Butterworth-Heinemann, Amsterdam

Katsikas S (2013) Risk management. Comput Inf Secur Handb:507–527. https://doi.org/10.1016/b978-0-12-803843-7.00034-x

Kurtz J (2017) Hacking wireless access points. Syngress, Amsterdam

Marr B (2018) Why the internet of medical things (IoMT) will start to transform healthcare in 2018. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#74b4d7504a3c

Marriott N (2017) Why the internet of medical things is the future of healthcare [Infographic, Video]. Retrieved from https://www.nexeonmed.com/media/why-the-internet-of-medical-things-is-the-future-of-healthcare

Mishra D, kumar S, Ashu A (2018) Internet of things: a survey on enabling technologies, application and standardization. SSRN Electron J. https://doi.org/10.2139/ssrn.3170749

National Cyber Security Centre (2018a) Homepage. Retrieved from https://www.cyberessentials.ncsc.gov.uk/

National Cyber Security Centre (2018b) Risk management and risk analysis in practice – NCSC Site. Retrieved from https://www.ncsc.gov.uk/guidance/risk-management-and-risk-analysis-practice

National Cyber Security Centre (2018c) 10 steps to cyber security – NCSC Site. Retrieved from https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

NIST (2018) NIST releases version 1.1 of its popular cybersecurity framework. Retrieved from https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Paul N, Kohno T, Klonoff D (2011) A review of the security of insulin pump infusion systems. J Diabetes Sci Technol 5(6):1557–1562. https://doi.org/10.1177/193229681100500632

Ray P (2016) A survey on internet of things architectures. J King Saud Univ Comput Inf Sci 30(3):291–319. https://doi.org/10.1016/j.jksuci.2016.10.003

Riahi Sfar A, Natalizio E, Challal Y, Chtourou Z (2018) A roadmap for security challenges in the internet of things. Digit Commun Netw 4(2):118–137. https://doi.org/10.1016/j.dcan.2017.04.003

Rivas H, Wac K (2018) Digital health: scaling healthcare to the world health informatics, 1st edn. Springer, Cham

Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. 2012 International conference on computer science and electronics engineering. https://doi.org/10.1109/iccsee.2012.373

The Chartered Society of Physiotherapy (2018) Big data is key to the future of the NHS, conference hears. Retrieved from https://www.csp.org.uk/news/2018-03-01-big-data-key-future-nhs-conference-hears

Trend Micro (2018) Blockchain: the missing link between security and the IoT? – Security news – Trend micro PH. Retrieved from https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/blockchain-the-missing-link-between-security-and-the-iot

Ulsch N (2014) Cyber threat!: how to manage the growing risk of cyber attacks, 1st edn. Wiley, Hoboken

Van Haren (2014) Global standards and publications. Van Haren Pub, [Place of publication not identified]

Yessad N, Bouchelaghem S, Ouada F, Omar M (2017) Secure and reliable patient body motion based authentication approach for medical body area networks. Pervasive Mob Comput 42:351–370. https://doi.org/10.1016/j.pmcj.2017.06.009

Zafari F, Papapanagiotou I, Christidis K (2016) Microlocation for internet-of-things-equipped smart buildings. IEEE Internet Things J 3(1):96–112. https://doi.org/10.1109/jiot.2015.2442956

Zhang M, Raghunathan A, Jha N (2014) Trustworthiness of medical devices and body area networks. Proc IEEE 102(8):1174–1188. https://doi.org/10.1109/jproc.2014.2322103

Zhou J, Cao Z, Dong X, Vasilakos A (2017) Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag 55(1):26–33. https://doi.org/10.1109/mcom.2017.1600363cm

Zhou W, Jia Y, Peng A, Zhang Y, Liu P (2018) The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J:1–1. https://doi.org/10.1109/jiot.2018.2847733