Consumer Awareness on Security and Privacy Threat of Medical Devices

Anthonia Sagay and Hamid Jahankhani

Abstract The Internet of Things (IoT) are being enthusiastically adopted by consumers. By the year 2020 the sum of 31 billon IoT devices will be deployed globally. Subsequent as the IoT device landscape is expanding at such speed, so does the threat landscape and vulnerabilities it introduces increases. Thus, making IoT devices easily prone to attacks or to be used to for launching attacks at large economical scale and society is seeing a growth in the scale and frequencies of these attacks. The large scale of attacks and frequency have caught global attention and causing governments to take the security and privacy threats of IoT very seriously and the UK government amongst others are now turning these concerns into actionable measures by considering ways of protecting consumers against the vulnerabilities and threats of IoT. It is part of these actionable measures that the NCSC (National Cyber Security Centre) recently published in a report about the new laws being proposed by the government to strengthen IoT devices. This chapter will look at the IoT security threats and privacy issues, it will explore whether the growing concern of the government to protect consumer has a foundation by investigating consumers awareness and attitude towards IoT security threats and privacy issues and propose a framework to facilitate the introduction of the new initiative of the government to bring in laws to govern IoT products thereby shifting the responsibility of the security threats to the manufacturers and away from the consumer.

Keywords IoT · IoMT · Privacy · Abuse · Cyber attack

A. Sagay · H. Jahankhani (✉)
Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-35746-7_6

1 Literature Review

The Internet of Thing (IoT) is a technological development phenomenon which is enhancing more and more ubiquitous connectivity around the world. It has succinctly eliminated the barriers in product design capabilities by allowing everyday basic devices to be internet-enable thereby adding significant value that were not previously possible or available to these devices. Consumer devices such as webcams, thermostats, watches, TV and many more now have internet capabilities and functionalities. According to J. Hou, L. QU and W. Shi (2019) IoT has enlarged the communication capabilities of Information Communication Technologies (ICTs) from "Any Time" and "Any Place" to "Any Thing".

IoT has introduced a connectivity paradigm of Machine-to-Machine (M2M), Machine-to-Man and Man-to-Man with identification management and control processes. The breath of IoT landscape is so vast and a typical architecture connects from front-end devices to back-end frameworks running in the cloud. Generally, this architectural landscape will include a significant number of smart devices, sensors that sense information from different environment and share them with cloud services for further processing (M. Aly, F. Khomh and M. Haoues et al. 2019).

The key role of the smart sensors in IoT is to assemble, measure and evaluate data and this function is what makes IoT so attractive and powerful as the measured data can be utilised to meet the requirements of any industry. Empirical research demonstrated that IoT offers the healthcare industry a great opportunity in refining operational adequacy, developing and enhancing patient care as well as promoting innovation. The healthcare industry bolstered as IoT made it possible to enable everyday device to provide intelligent data wherever and whenever simply by attaching these devices to the patient; information can be gleaned unhindered by any network or services. By building sensors into these simple things which are then embedded/worn in or on the body the healthcare industry can gather enormous amount of data about patient's health status. Having access to data in this manner opens new possibilities for the healthcare industry and radicalised treatment offered to patients and reduces the care of cost with enhanced results. However, all of these introduces multi-level complexity as more vulnerabilities are introduce creating severe security challenges across the IoMT landscape.

1.1 Security Threats and Privacy Issues of IoMT

The Norwegian research organisation SINTEF reported that in the past 2 years, 90% of the world's data has been produced at a speed exceeding 205,000 gigabytes per second and this was approximated to the equivalent of 150 million books. The data collection of IoT spans the healthcare, retail, transport, manufacturing and many more industries for which IoT can provide smart services by extracting valuable information from diverse collection of data at the IoT end-point devices, which has

significant impact on social production and people's life. Base on the important role that data plays in IoT, it can be inferred that discussing IoT without considering data is incomplete. The healthcare IoT market is expected to reach $117 billion by 2020 according to market research. This rapid growth of IoMT has raised considerable concerns around disclosure of personal privacy information particularly around sensitive medical data.

According to an article published by the British Medical Journal in July 2017 the Healthcare sector is more susceptible to cyber-attacks than other sectors owing to the inherent weakness in its security position. The article stated that it is one of the most targeted sectors globally. Amongst the 223 organisations that participated in the survey 81% were from the medical sector and over 110 million patients in the US had their data compromised in 2015 alone. Furthermore, only 50% of the providers were confident that they could defend themselves against cyber-attack and record shows a 300% increase in attacks in the past 3 years. The health sector is an attractive target for two reasons: it offers a rich source of valuable data and it is an easy target. Data is at the core of IoT so much so that researcher are inferring that just as monitoring blood in the human body provides valuable insights into people's health, observing data in an IoT environment could provide significant insight into the security of IoT. Evidently the healthcare sector is a storehouse of valuable data and according to the British Medical Journal another primary reason it is targeted is for financial reward and benefits owing to the nature of the data that can be gleaned. The sum of 80 million records were stolen from Anthem, a US health insurance company and the monetary value of this data on the dark web was estimated to range in billions of dollars. Unlike credit card data that can easily be reset, an individual's medical record could contain sufficient information for a perpetrator to open a bank account, obtain loans or acquire a passport basically fully cloning the victim's identity.

1.2 Recent Cyber-Attacks on Health Sector and the IoMT Threat Landscape

In May 2015 according to the BMJ (British Medical Journal) there was a global cyber-attack unleashed in form of the WannaCry Ransomware; although this attack was not specifically targeted at the healthcare sector and affected around 200,000 systems in more than 150 countries according to the reports. An estimate of about 50 hospitals in the UK were directly hit by the WannaCry Ransomware attack whilst many more in anticipation shut down computer systems causing considerable disruption, impacting the delivery of care, jeopardising patient safety and potentially eroding trust.

In 2016 the Hollywood Presbyterian Medical Centre was compromised due a ransomware attack causing it to shut down its network for 10 days resulting in staff not having access to medical records or being able to use medical equipment until

the ransom was paid. The cost of this attack was estimated at $17,000. Another ransomware incident also reported in 2016 was an attack on an English hospital and the impact meant all operations were mandatorily cancelled and patients were transferred to other facilities for 2 days. Freedom of Information request in the UK reported that between the years 2015–16 around 50% of NHS trusts were affected by ransomware in the preceding year. The Australian Red Cross Blood Service reported a breach in 2016 which resulted in the publication of 1.28 million records with large amount of sensitive data, including donor's at-risk sexual behaviour on a public website.

According to a recent article published by Fortinet cited by Adefala (2018) as the healthcare sector technology (IoMT) grows, so does the cybersecurity attack surface. Frost and Sullivan forecast that by 2021 IoMT will reach a growth of $72.02 billion with over 30 billion connected medical devices in the healthcare ecosystem [7]. IoT has transcend the medical sector by introducing numerous IoMT-based platforms, applications and services that enabled remote health monitoring, fitness programs, chronic diseases and elderly care. Guan et al. states that IoMT offers unconventional solutions to the challenges of traditional medical system such as lack of doctors, health resources and research data. In addition, the rapid development has enhanced traditional medical systems in diverse areas, such as disease diagnosis and analysis. Furthermore, the health data gathered in IoMT enables researched to diagnose and predict diseases.

The attractiveness of IoMT combined with its terminal devices is causing exponential growth in the data collected. With the endless possibility that IoMT is offering the healthcare sector, it growing popularity is understandable. Notwithstanding this rapid and excessive growth is a major contributing factor in the expansion of the attack surface making it extremely difficult to address using traditional devices and strategies. Hence the urgent need for cybersecurity to protect the confidentiality, integrity and availability of valuable healthcare data.

The futuristic trend of IoT has not only successfully revolutionised the healthcare sector but has also enable a complete merger of the cyber world to the physical world to create what researchers are calling the cyber-physical world. Due to the cyber-physical nature of IoT, there is a need to consider the security of IoT from a unified perspective by considering both safety and security. Wolf and Serpanos [10] introduced the concept of considering the cyber-physical characteristics of IoT in view of a unified security model from the perspective of safety and security. Unquestionably, IoMT can be classified as a safety-critical cyber-physical system because it comprehensively considers both the reliability and safety of conventional medical devices, as well the dynamics and generic nature and the scalability capabilities of traditional IoT. IoMT devices are designed to constantly interact with the physical world.

Therefore, it can be inferred that safety and security should be considered as a critical challenge for IoMT especially given the severe consequences of an attack and the extensive attack surface. The physical devices in the IoMT infrastructure are embedded with sensors to form a connected ecosystem which is then tagged around

the patient to capture, measure and identify key data; stratify risks; make decisions and initiate the necessary action plan. These sensors and controller embody the communication bridge between the cyber and physical world which ironically are major contributors to the vast security threats and privacy issues facing IoMT landscape. These sensors and controllers utilise applications available on phones or web therefore, from a security perspective these devices are susceptible to attacks and exploit in the same manner as a traditional endpoint device such as desktop computer.

Thus, once an attacker can identify a vulnerability, the damages could range from taking total control of the system, accessing and altering the data, flooding and overwhelming the system; the possibilities of malicious attacks are endless. Nevertheless, there are some significant differences that must be considered for IoMT security over traditional technology. Firstly, the accelerated adoption of IoMT has been identified by existing research to pose great security threat and privacy issue owing to the absence of proper security guidance, a landscape of uncertain liability, new standards and emerging polices and regulations.

Typical example of the landscape uncertainty was identified in a recent article on the Metro published in July 2019 regarding the ownership of digital footprint in the event of the death of an individual. The article reported that according to Survey conducted last year by YouGov only 7% of participant consented to keep their social media account active upon their demise, although another study by Oxford Internet Institute (OII) approximated that by the year 2100 the number of dead people whose account will still be active on Facebook will be 4.9 billion. There is now a debate around the ownership of data upon the death of an individual and the question of who should own the data. Should it be Facebook or the deceased family and friends.

Craig Badrick reported in his article publish in January 2019 that the FDA (Food and Drugs Administration) estimated that for over 1000 IoT devices in use 164 are subject to attacks. Subsequently as the hospitals introduce more and more applications for IoMT they risk the likelihood of introducing devices that may put their operations and patient's life in jeopardy. Arguable manufacturers must be made accountable as currently majority of the IoMT devices are not specifically optimised for hospital security network. Regulators such as FDA and other industry standards are falling behind the times and only 17% of medical manufacturers have been reported to be taking steps towards preventing attacks. Given the severity of the nature of the risk and what it is at stake it is shocking to report that security attributes in IoMT devices at unreliable at best. It is common place to find an IoMT with unencrypted communications, weak or non-existent password protection, or setup that make it more problematic or impossible to patch the device for improved security.

The IoMT threats are grave as it impacts both individual patients as well as the entire hospital system. 2017 recorded the recall of 465,000 pacemakers owing to a report that they have been hacked putting patients' lives at risk. In addition, another case reported that about 95% of healthcare institutions have at some point been targeted. Another incident reported in 2015 by the Health and

Human Service Office of Civil Rights that 112 million health records had been breached or compromised in that year. The compounding evidence calls for urgent standardisation across the IoMT ecosystem infrastructure and an intervention with clearly defined accountability for both the manufacturers of devices and those using the device.

1.3 Characteristic of IoMT Comparable to IoT and Cybersecurity Requirements

The IoT landscape is very broad and as such the consultation and the consultation-stage impact assessment set out to define consumer IoT products and included in the examples produce was wearable health trackers which falls under the IoMT category and is the focus of this study. Hence the need to consider the characteristics of IoMT comparable to IoT in other to ascertain if a single framework can be applied across board as best practice with the flexibility for manufacturers and organisation to make adjustments suitable to their environment or perhaps a distinct framework may be required for IoMT.

The interconnection of IoMT are not limited to personal medical devices but it extends from devices to healthcare providers such as hospitals, medical researchers or private companies. Furthermore, existing research identifies that personal smart product are generally wearables it is therefore understandable that the DCMS consultation document has identified and defined IoMT under this category. Gatouillat et al. suggest that owing to the strict ethical concerns of the medical community, biomedical devices must adhere to the following three requirements:

1. Reliability – the expectation here is that the functional goals of the system must always be reliable and should not be susceptible to abrupt failures under normal operating conditions. Fundamentally, the potential diagnostic nature of IoMT-based systems puts reliability at the core of every system component to ensure the correctness and validity of information collected.
2. Safety – this implies that a safe system ought not to cause harm to its operating environment therefore IoMT particularly in the context of medical actuators concrete evidence should be available to ascertain that the system will not cause harm to its user.
3. Security – Medical systems ought to be unyielding against external threats and attacks particularly owing to the sensitive and personal nature of the information they accumulate.

According to Alsubaei et al. [1, 2] the healthcare industry has the highest number of IoT devices; ranking at about a third of all IoT devices and this number is expected to increase by 2025 which will make healthcare the largest sector dominating the IoT device market with an estimated percentage of around 40% of the total global worth of IoT technology ($6.2 trillion). The uptake of IoT in the healthcare sector is unprecedented and currently the number of organisations in the healthcare sector that have adopted IoT technologies is approximated at 60% and this is expected to increase to 87% by 2019.

Based on the extraordinary growth, evolution and dominant of IoMT technologies the evidence suggests that there is an urgent need to address the security threat and privacy issues in this sector especially when the consequences range from severe impact on patient's wellbeing, damaging outcome on medical data privacy, brand reputation, business continuity and financial stability. Furthermore, the array of complexity as identified by Jalali and Kaiser [7] including the dearth of consensus amongst internal stakeholders on security requirements, the disparate technology environment couple with the complexity of multiple channel of IT technology acquisition, internal politics complicated by the intricacies of functions contained within the organisation and additional regulatory pressure. Thus, this study will focus on proposing a framework for IoMT devices that support the implementation of the new laws being proposed by the government.

1.4 Fundamental Objectives of the DCMS Proposed New IoT Security Law

DCMS commission Harris Interactive to conduct a consumer IoT (Internet of Things) security labelling survey in March 2019. The survey identified that consumers have a complacent attitude toward seeking out security information about their smart devices. According to the survey 72% of the respondents naively assume that security features are built into these devices as a default. To alleviate and manage the unprecedented consumer assumption which poses a risk not just to the consumer but the wider economy at large the DCMS are mandating IoT device manufactures to introduces labels that clearly highlights and outlines the security features of a device to help consumers to be better informed about the security attributes of smart devices when making purchase. Subsequently these labels aim to reinforce consumers confident by emphasising that devices meet security standards and provide information on the minimum period for manufacturer security updates. The images below represent the draft design for proposed label at this initial consultation stage. Although there are still concerns and other issues surrounding this design, but these discussions are outside the remit of this study (Fig. 1).

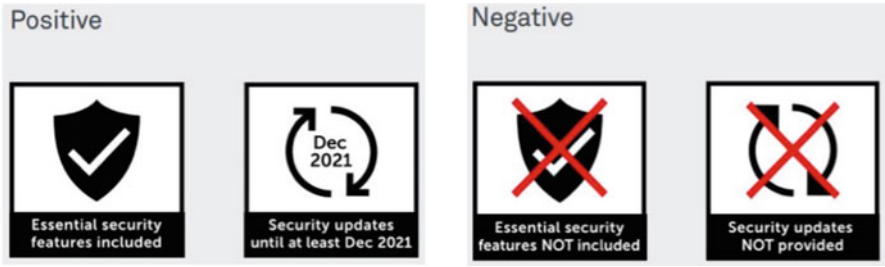

Fig. 1 Draft design of the DCMS IoT security label

1.5 Best Practice and Framework Consideration for Cyber Security Comparable to the New IoT Law

Robert Meyer an expert in assessing the relationships between frameworks proposed in his presentation (November 2016) the core values of Information Technology frameworks. According to Meyer IT frameworks can offer the following:

- Better value creation through effective and innovative use of enterprise IT
- Increased business user satisfaction with IT engagement and services
- Increased compliance with relevant laws, regulations and polices
- Improved relationship between business needs and IT objectives
- Increased financial return from the governance over enterprise IT by obtaining the greatest value from investments in technology
- Connection to, and where relevant alignment with other major frameworks and standards in the marketplace

Information Technology has been described as ubiquitous and critical for business matters within companies, between interconnected companies and/or private individuals for cloud computing solutions, Internet of things, connected and mobile devices and many more internet usages. Due to this indispensable nature of IT risk management has become prevailing [3]. Essentially risk management activities within all domains ought to be under control either for dedicated risk management purposes or for a broader perspective in management systems. Hence the domain focus of this study IoT/IoMT must adhere to risk management controls.

Significant amount of the discussion of this chapter has been centred on the security and privacy risk of IoT/IoMT and according to Brenner [3] there is unquestionable ties between information security and risk management therefore the proposed framework to facilitate the implementation of the new IoT security law will be anchored on best practice standard(s).

SO/ICE 27001 provides a set of guidelines and requirements for developing and implement an information security system and it has controls built in that ties it closely to risk management. In addition, this standard takes an agnostic approach for any specific technology offering the organisation the opportunity the best and

most practical controls for their organisation [3]. Pulling this back into the context of this study one of the key requirements of the proposed new IoT security law is that manufacturers still have the flexibility of innovation whilst implementing the appropriate security solutions on the devices.

This standard has been selected specifically based on its relevance to the discussion of this study; also, having established that one of the advantages of standard and framework is the flexibility to align and synergise guidelines and controls to form a robust solution. Furthermore, the selected standard is agnostic in its approach but comprehensive in providing controls around risks and security management.

ISO Standards are common place in today's business world as acceptable standards for benchmarking and identifying organisations who follow best practice. Typically, frameworks are designed to be adopted and tailored to an organisation needs in terms of policies, procedures, industry and/or services rendered. Much of the discussions in this chapter thus far have focused on the security and privacy risk of IoT and as such the framework proposed will consider various aspects of Risk and Information Security Management thus the following ISO standards will be considered for inspiration; ISO/IEC 27001 – Information Technology Security Techniques and Information Security Management Systems Requirements; ISO 13485 Medical Devices – Quality Management Systems and Requirements for Regulatory Purposes; ISO/IEC 30161 Internet of Things – Requirements of IoT data Exchange Platform for Various IoT Services and BIS 31000 International Risk Management Guidelines [9]. NIST IR 8228 will also be considered because it covers Cybersecurity and Privacy Risk for IoT and offers some useful hierarchical structures for identifying/grouping of attack vector surface as well as a good construct of how to mitigate the risks. Furthermore, the scope of this study is around IoT Security and Privacy threats that affects consumers and the guidelines proposed in the NIST IR 8228 is relevant to the objective of this study. Reference will be made to other types of risks that should be considered alongside the Security and Privacy threat focus of this study including safety, reliability and resilience owing to the nature of the knock-on effects that isolation of one risk can have on other risks.

2 Users Profiling and Smart Device Usage

Harris Interactive conducted a study on behalf of the DCMS which reported that 72% of the participants believed that security features were built into smart devices by default whereas the government are on a mission to protect consumers after having identified that majority of the smart devices in the public market domain do not even meet basis security requirements. Evidently there are discrepancies in these two camps.

This study intends to examine consumer awareness and attitude towards security threats and privacy issues of IoT in other to highlight the urgent need for the education of the consumer. In addition, the study will investigate the ongoing efforts

of the government to protect the consumer against the security and privacy risks of IoT. To conduct this investigation a quantitative, descriptive questionnaire survey was used as a primary data source and literature reviews as well as government consultation and legislative documents as secondary data source [8]. The questions were designed using an online survey tool as it offered simple but professional looking user-friendly design, provided different medium to distribute survey to participants and collates all the responses in a central location. Most important of all it allowed respondents to remain anonymous and saved resources in terms of time and money.

The audience targeted to participate in the questionnaire survey were between ages 16–65 that owned some form of smart device. Participants were randomly selected as the basis of the study is to identify the topic from the perspective of the general public. A total of 256 participant received a web link to the questionnaire via social media platforms such as LinkedIn and Facebook. Friends and family were also approached to participate in the experiment and were encouraged to share the link to others in their social network to diversify and ensure that the generalist criteria of the required responses are adhered to.

Quantitative research method was selected for this study because it focuses primarily on numerical data and interprets this information using statistic under a reductionist, logical and strictly objective paradigm. Traditionally social science research often utilises existing completed studies in form of literatures that relates to or addresses the hypothesis [8] cited Spyros Konstantopoulos). Thus, narratives gleaned from existing research contributed significantly in designing the survey questions to establish status quo on consumer's awareness and attitude towards security threats and privacy issues around IoT. Questions were constructed to examine the following four areas:

- Consumer awareness/knowledge of the concept of digital footprints
- Consumer smart device security awareness
- Consumer awareness of the potential damage that a security or privacy breach can cause
- Consumer priority preference of smart device benefits versus security and privacy concerns

The survey comprised of 32 questions and was disseminated to 256 participants of which 133 responses were received.

As previously mentioned, secondary data in form of literature review contributed significantly to the findings of this study. The secondary data reinforces the concerns in the dearth of awareness of consumers on the topic of security threats and privacy issues of IoT. Evidence of this was derived from an existing research conducted by Harris Interactive in February 2019 which revealed that consumers have a complacent attitude towards seeking out security information about their smart device and 72% of respondents innocently assumed that security features are built in to smart devices by default. Another secondary data which also strengthened the argument of the study was taken from a survey conducted by Internet Society in May 2019 which reported that consumers have serious concerns about the security

of their smart devices but are not knowledgeable about how to adapt and adjust device settings in a manner that might deter these fears.

Ethical consideration has become critical particularly on the recent entrance of GDPR regulation. Therefore, in a bid to ethically align this study the following considerations were considered. Scope of study was clearly defined, and all participants were provided with explicit explanation of the purpose to which the data is being collected and how it will be used prior to the collection of the data. Furthermore, participants were informed that all data collected will be used specifically and solely for the purpose of this research after which the data will be destroyed once the findings of the research are concluded.

The questionnaire survey was conducted in July 2019 and contained 33 questions. Two hundred and fifty six people received the weblink to complete the questionnaire. Respondent age group were between 16–65. About 99% of the total participants indicated that they owned smart devices from popular brands. The brands listed were Apple (58% of respondents), Samsung (43% of respondents), Microsoft (11% of respondents), Huawei (9% of respondents), Fitbits (10% of respondents) and other less popular brands (15% of respondents). Sixty-two percent of respondents confirmed that they actively engaging with the smart features on their smart devices, whilst 38% report that they do not actively engage with the smart features on their smart device. Eighty-eight percent of respondent confirmed that they engage with the smart features of their smart device via their mobile phone, 4% reported they use their tablet and 7% engage via their laptop. Respondent reasons for not engaging with smart features on smart device were (a). Too complicated (13%), (b). cannot be bothered (37%), (c). see no benefits (12%), (d). concerned about security (13%) and (e). concerned about their information (23%).

2.1 Understanding the Consumer Awareness

This study is conducted to understand the consumer awareness on the implications of their interactions and usage of their smart devices. To that end respondent were asked the importance of the benefits they derive from the information receive from their smart device. Fifty-two percent responded that the benefits are important, 33% agreed that the benefits are somewhat important, 12% reported that benefits are not important. The survey results revealed that 62% of respondent understand the term "digital footprint" whilst 38% do not understand the term. Furthermore, 79% of respondents stated that they are aware of the possibilities of leaving a digital footprint trail whilst 21% reported are not aware that their interactions with the smart features on their smart devices leaves behind digital footprints. When asked about the type of digital footprints, social digital footprint had the highest level of awareness amongst respondents at 80% and financial digital footprint was second at 70%, medical digital footprint came third at 39%, then economic digital footprint 24% reported they were aware of this, 22% confirmed they were aware of environmental digital footprint and 20% stated they are aware of biological

digital footprint. These findings are an indication that there is a degree of awareness amongst consumer about the different types of data and information trail that are left behind as a result of their interactions and engagement with their diverse smart devices, but this is not enough evidence to ascertain if consumers understand the implications of what this translate to, neither does it reveal the consumer reasoning regarding safety awareness when engaging with their smart device. To put this in context if we look at cigarette pack the message "Smoking Kills" is clearly inscribed on the package and there is enough information as well as awareness on the dangers of cigarettes. The responses gleaned from the findings of this study indicates that more in terms of educating consumers about security and privacy considerations when interacting and engaging with their smart devices is required.

2.2 Consumer Security Awareness

The study other objectives included ascertaining consumer security awareness and attitude whilst interacting with the smart features of their smart devices and to this end consumers were asked if they were aware that most smart device have default password. The findings were as follows: 54% of respondent stated that they are aware that their smart device has a default password and 46% reported that they were not aware that their smart device has a default password. Respondents were asked about their awareness regarding the need to change the default password on their smart device regularly and the findings reported that 68% of respondent were aware of the need to change the default password on their smart device regularly, whilst 32% stated that they were not aware of the need to change the default password on their smart device on a regular basis. Another consideration was to ascertain if respondent know how to go about changing the default password on their smart device and the findings reported that 63% of respondent know how to change the default password on their smart device, whilst the remaining 37% do not know how to go about changing the default password on their smart device. On the final aspect of the security awareness and attitude, respondent were asked if they are likely to read security instructions if it were to be included in their smart device when they purchased it and the findings showed that 42% of respondents are likely to read the security instructions, 24% are indifferent so they are neither likely or unlikely to read security instructions, 32% are unlikely to read security instructions included in their smart device upon purchase. These findings reinforce the findings from the previous section that consumer need to be educated on the seriousness of security threats and privacy issues regarding their smart devices. The evidence clearly indicate that consumers lack awareness and have a complacent attitude around safety and security when interacting with the smart features on their smart device.

2.3 Benefits Versus Security and Privacy Concerns

Another objective of the of the study was to understand consumers attitude towards the benefits derived from their smart device versus their concern over security and privacy breach as a result of their interaction with their smart device. Respondent were asked a series of questions and the survey results revealed that 82% of respondents are aware that a security and privacy breach of their smart device can impact others across their network and 18% of respondent were unaware of this. When asked about attitude about their digital footprint being captured in a remote location as a result of their interaction with smart device, the result showed that 24% agreed that they would be concerned about this, 19% were indifferent, 57% of respondents disagree that this would concern them. Respondents were asked about the importance of their smart device to their every-day life and results revealed that 68% agree that their smart device was critical, and they cannot do without it, 24% were different about the importance as they neither agreed nor disagreed and 8% disagreed that their smart device was critical to their life. When asked about their attitude toward the use of their data by smart device manufacturer, 70% of respondent agree that they will make an effort to understand how their data is used by smart device manufacturer, 22% were indifferent about how smart device manufacturers use their data and 8% of respondent disagree that they would be interested in how smart device manufacturers used their data. Further probe about the use of their data reveal that 70% of respondents agree they would make an effort to get clarification on the use of their data if they do not fully understand something, 20% of respondent were indifferent and 6% of respondent disagree that they would make an effort to get clarification on the use of their data if they do not fully understand something. When asked about the importance safeguarding their digital footprint over the benefits derived from smart device, 68% of respondents agree that safeguarding of the digital footprint is more important than the benefits derived from their smart device, 25% of respondents were indifferent about the safeguarding of the digital footprint being more important than the benefits derived from their smart device and 4% disagree that safeguarding of the digital footprint is more important than the benefits derived from their smart device. When asked about their understanding of the consequence of a security or privacy breach, 81% of respondent reported that they fully understand that a security or privacy breach could lead to minor or colossal fatalities, 12% were indifferent about their understanding of the consequences of a breach and 7% reported that they do not fully understand the consequences of a breach. 44% of respondent revealed that prior to taking part in this study they did not consider security or privacy as a concern when acquiring smart device, 19% revealed they were indifferent about their consideration of security and privacy when acquiring smart device prior to this study and 34% stated that they do consideration of security and privacy when acquiring smart device prior to this study. When asked about their attitude about security and privacy going forward after participation in this study 83% of respondents stated that security and privacy will certainly be a consideration henceforth when acquiring smart devices,

14% were indifferent about what they whether they will consider security and privacy when acquiring smart devices after having taken part in the study and 3% of respondent disagree to consider security and privacy as part of selection criteria for acquiring smart devices even after taking part in the study [5].

The evidence and findings of this study shows that consumers do appear to have a degree of concern about security threat and privacy issues around IoT smart devices, but the finding also revealed conflicting attitude between consumer security and privacy concerns and the benefits derived from their IoT smart device. Furthermore, the finding of this study aligns with findings from studies conducted by Internet Society and Harris Interactive. Both studies identified that consumers do have genuine concerns about security and privacy when it comes to IoT smart devices and the Harris Interactive study clearly identified consumer complacent attitude to seek out knowledge for themselves and educate themselves to improve their basic awareness on what security and privacy consideration should be considered when acquiring IoT smart devices. The Internet Society also reported in their study consumers are concerned about security and privacy, but they lack the know-how on how to adapt and adjust their device settings to alleviate these fears and concerns. Based on these findings it can be inferred that there is a need for government intervention and the consequently the government are already gearing up to address this issue as a matter of urgency as previously identified in this study.

3 IoMT Cybersecurity Framework Design

Alter (2003), Bunge (1985) and Simon (1996) suggest that information systems designed to support organisations are complicated, artificial and purposeful. The common composition of this design includes people, structures, technologies and work systems. For this study the Hevner et al. [6] Information Systems Research Framework diagram below will serve as a guide to design the proposed IoMT Security and Privacy framework (Fig. 2).

The illustration above is presented by scholars as a conceptual framework designed to aid the understanding, execution and evaluation of IS research merging behavioural-science and design-science paradigm. The framework serves as a tool used to position and compare these paradigms. The Environment according to Simon (1996) describes the problem space where the phenomena of interest resides. Silver et al. (1995) suggest that the environment is made up of people, (business) organisation plus their existing or planned technologies. Therein lies the definition of the goals, tasks, problems and opportunities that the business need from the perspective of the people within the organisation. These perceptions are influenced by the roles, capabilities and characteristics of the people within the organisation. Furthermore, business needs are identified by assessing and evaluating the context of organisational strategies, structure, culture and existing business processes. All the above-mentioned are then positioned comparatively to current technology infrastructure, applications, communication architectures and development capabilities.

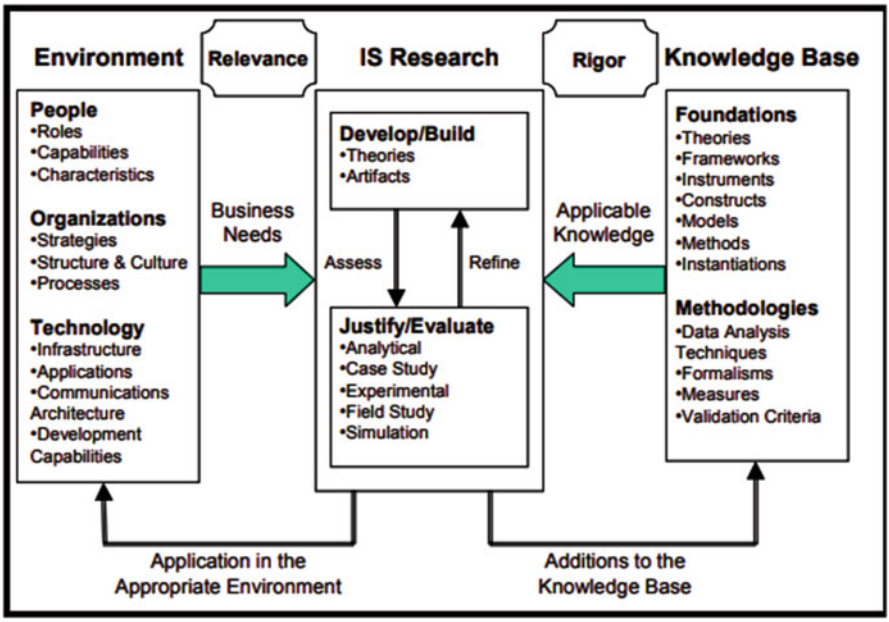

Fig. 2 Information systems research framework. (Source: Ref. [6])

The summation of all these essentials contributes to defining the business need or "problem" from the researcher perspective [6]. Thus, framing research activities to deal with the business needs gives credibility and relevance to the research.

The bedrock of IS (Information System) framework design according to behavioural and design science is a combination of people, structure, work system (processes) and technology as illustrated in the IS conceptual framework diagram in Fig. 3. Thus, IS conceptual framework will be used as the building block for the proposed IoMT framework for this study. The IoMT Security and Privacy Framework is designed to introduce structure to the key areas that have been identified to represent vulnerability bottlenecks within the healthcare sector.

3.1 Management Information Systems

The IoMT Security and Privacy framework provide a holistic view to support all cross functional and inter-organisational business processes and this will be supported by robust Management Information system that will outline succinct business outcomes including adequate measures and controls. These management systems will include the organisations acceptable risks tolerance and prescriptive actions for managing risks at different levels. The information systems inculcate the governance of information security management across all the management

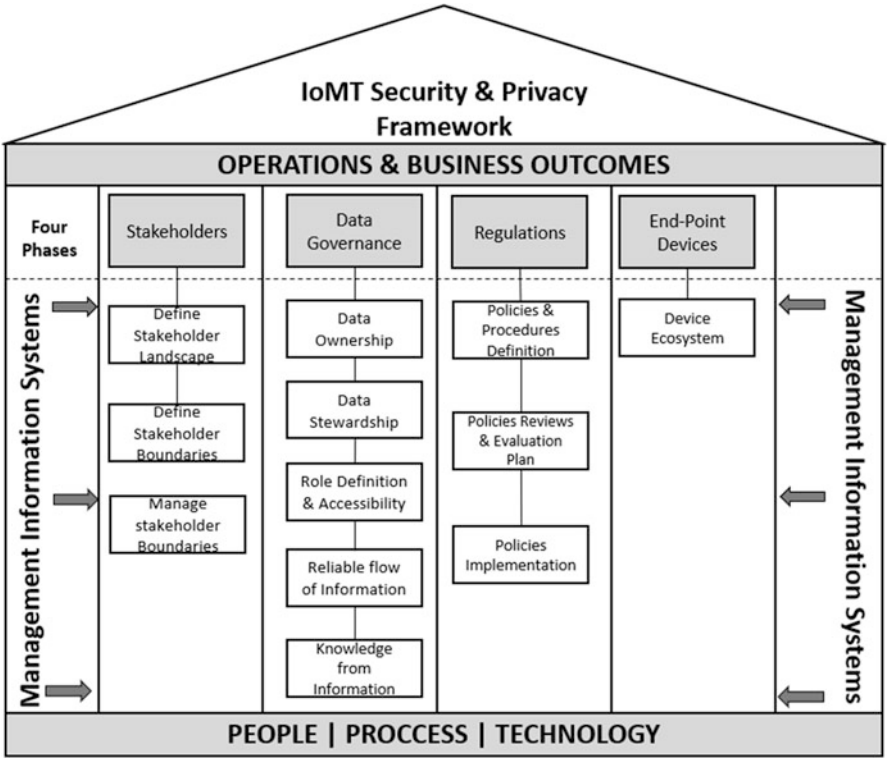

Fig. 3 IoMT security and privacy framework. (Source: Sagay A)

systems and define policies. It will also cover risk management adopting the agnostic characteristic of ISO27001. The ISO27001 standard dictates that security policies must be clearly define and documented procedures must be in place for assessments and treatment of risk. The management Information system represents a holistic perspective and as such the overarching security governance must be all encompassing therefore the Information security Governance Framework will be considered as a good fit to reinforce and ensure a robust security and privacy environment across functions and business activities (Fig. 4).

3.2 Stakeholder

Stakeholders are the people that have a keen interest and/or affected by activities within the organisation or more specifically the healthcare sector. Different stakeholders have different needs and requirement and as such it is important to define the different types of stakeholders by mapping out the entire high-level

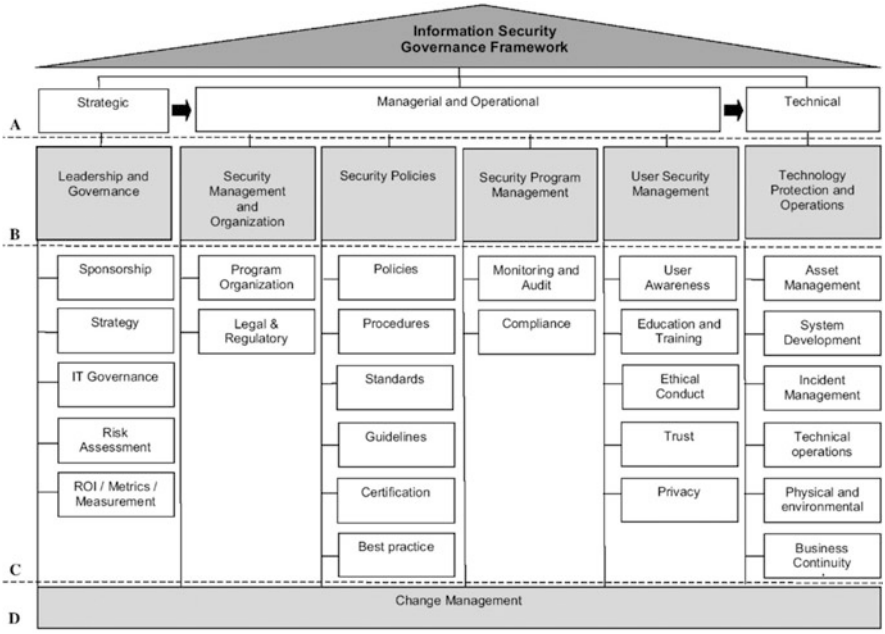

Fig. 4 Information security governance framework. (Source Veiga, A. D. and Eloff, J. H., 2007)

view of all stakeholder landscape that will be affected by the diverse activities and functions across the organisations. The above-mentioned will be handled by the Define Stakeholder Landscape step. Another aspect that will need to be considered is the definition of the different roles and level of involvement for the different stakeholders this will ensure expectations are properly managed and a good governance process across the entire stakeholder management process. This later part will be handled by the Define Stakeholder Boundaries step and will include detailed stakeholder matrix. The dynamic of business activities can cause the role and level of stakeholder involvement to change and as such there needs to be adequate process and controls to manage these changes. This will be handled by the Manage Stakeholder Boundaries step.

3.3 Data Governance

Data is the key commodity of the healthcare sector and represents the focal point of target of cyber-criminal activities and must be protected at all cost. Good data governance guarantees secure accessibility to top quality data that allows integrated data-driven decision making resulting in measurable outcomes [4]. Five key principle have been identified for the successful implementation of a robust data

governance solution and they include: Data Ownership, Data Stewardship, Role Definition and Accessibility, Reliable Flow of Information and Knowledge from information.

3.4 Data Ownership

Data ownership is primarily about accountability, responsibility and conduct around the organisations data. It set out the guidelines, standards and best practice of data management within the organisation. The underlying focus is ensuring behavioural control measures are in place outlining the correct definition, production, organisation and use of information. Given the IoMT data are stored in the cloud the policies will need to include controls and measures to manage data stored in the cloud.

3.5 Data Stewardship

Data stewardship is concerned about the quality of data and is centred around industry standard Data quality framework. The framework is an iterative process and supports collaborative working which promotes transparency and helps to achieve the benefits of good quality data. Data quality is an essential requirement for making data informed decisions (Fig. 5).

3.6 Role Definition and Accessibility

Privacy, compliance and security are defined under role definition and accessibility. The healthcare sector operates an inherent risk environment owing to the sensitivity of the data hence why data governance is integral to the industry. Ensuring that adequate risk management strategies and embedding risk awareness culture within operational activities is paramount [11]. Furthermore, alignment with other business functions such as record retention compliance requirement will result in a successful and robust data governance.

3.7 Reliable Flow of Information

Good data governance needs to have a solid Information Architecture and Integration that will promote and support the standardisation of common data definitions and ensure these definitions are made available across different platform resulting in good and well-informed decision making. The benefits of having common data is

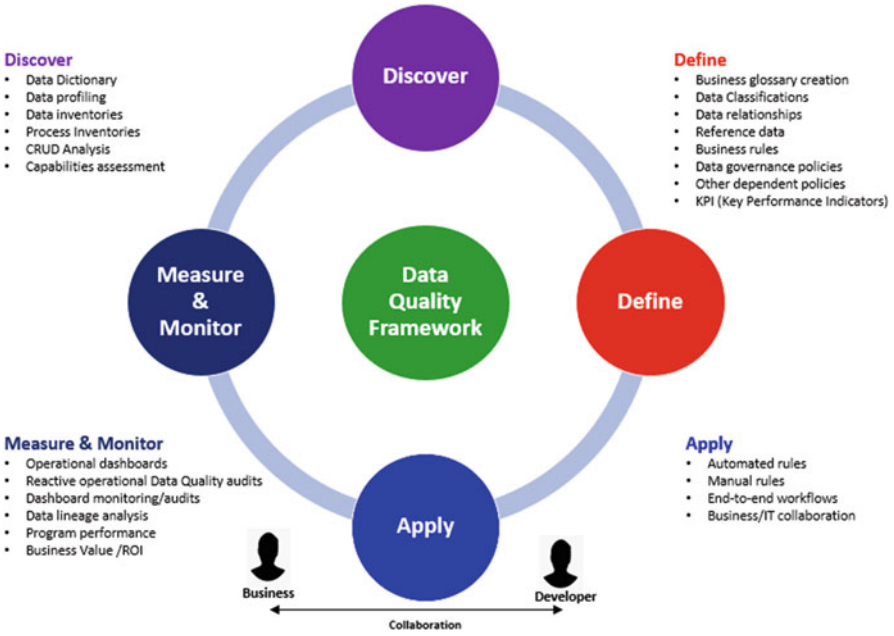

Fig. 5 Data quality framework. (Source: Sullexis Consulting)

that it can be utilised in multiple locations to define current and future capabilities within the organisation, design a durable architectural ecosystem and encourage organisation wide data integration.

3.8 Knowledge from Information

Organisation are heavily reliant on their body of data knowledge especially in the era of big data where data represents competitive advantage and as such reporting and analytics of organisation business data is critical for informed decision making. Data is at the core of all healthcare section activities and the entire IoMT ecosystems extrude data and as such a good measure of quality control will need to be put in place.

3.9 Regulations

Legislative and compliance requirements help organisation to promote and incorporate best practice across functions and business activities. The healthcare sector is

heavily regulated, but majority of its legislation focus on patients care and licensing requirement for medical personnel. The risk landscape is constantly changing and there is an urgent need for a culture change within the healthcare sector because cyber security responsibilities can no longer be considered as a problem for the IT department. NIST DES (Data Encryption Standards) Standards offers guidance and best practice relevant to the primary commodity of the healthcare sector. Specifically emphasising the importance of cryptographically protecting sensitive and/or valuable data against disclosure or undetected modification during transmission or whilst it's in storage. A good regulatory framework provides well defined Policies and Procedures and must be embedded within the core activities of the organisation. Regular Reviews and Evaluation of Policies and Procedures will result in a culture change and remove the danger of treating Cyber Security risk as a one-off independent activity and a good Plan for the Implementation of Policies will reinforce and send a message across the organisation of its priority and importance.

3.10 End-Point Devices

The threat landscape of IoMT is vast and growing rapidly especially the end-point devices. The discovery or implementation of any solution to a problem requires an in-depth understanding of the complexity and challenges of the problem environment in other words IoMT Security cannot be planned for, monitored, managed or controlled if the complexity and challenges are not identified and fully understood. The FDA (Food and Drug Administration) defines IoMT end-point devices as "Instruments, apparatus, implement, machines, contrivance implant, in vitro reagent, or other similar or related article, including a component part or accessory intended for use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease". Thus, a discovery and identification of data communication and transmission between end-point devices and other component within the IoMT infrastructure can offer valuable insight for a robust security solution.

3.11 Device Ecosystem

According to the Global System for Mobile Communication Association (GSMA) endpoints are physical computing devices responsible for performing motoring activities such as detecting, and it operates as part of an internet-connected product or services including wearable devices. Typically, endpoint device will also connect to hospital networks as well as other medical devices. The end-point communication ecosystem provides transparency by creating visibility potential data entry and exit points for greater control and traceability. Furthermore, this transparency will

provide insights for tailored security consideration as one sight cannot fit all given the complexity and disparate nature of the requirement of the healthcare sector.

3.12 People, Process and Technology

Achieving the benefit of good and effective governance cannot be a one-time exercise or activity but rather a continuous cyclical and iterative process that is executed by people and overseen by robust and well-defined technology solutions. The Healthcare sector is complex in its diversity and as such adopting a one size fits all security solution presents a challenge. The model is built on three principles:

- Ontological approach gives autonomy and singularity to its object and still allows the object qualities to exist independently.
- Centred around stakeholders by considering the disparate security requirements and responsibilities of stakeholders within the healthcare sector. The diverse roles mean that different stakeholder's (Patients, Medical Professionals and System Administrators) need will require a different type of interaction with the solution.
- Scenario-based concept considers the heterogeneity of the IoMT device landscape which will also require solutions to be considered according to the business security requirements.

4 Conclusion

This study has proposed an IoMT Security and Privacy Framework based on the key concept of design science paradigm of people, processes and technology in addition to adopting as well as adapting existing best practice standards that are in alignment with the objectives of the framework. Discussions also included the attractiveness of high-level security and privacy breaches of healthcare sector for criminal due to the financial gain and the patient centric nature of the industry means its lagging behind in cybersecurity expertise therefore making it an easily accessible target. In addition, it discussed the unique security and privacy challenges of IoMT particularly homing in on the complexity of the diverse stakeholder security and responsibility requirements and the challenges of the heterogeneity of end-point devices making the idea of a single solution of one-size fits all not advantageous for this environment. Having discussed and considered all of these things the IoMT Security and Privacy Framework was then created with emphasis on data governance because it represents the most valuable commodity within the healthcare sector, stakeholders as they are responsible for executing activities within the operational environment and unique processes tailored and designed to meet the diverse security and privacy requirement as dictated by the environment as well as the stakeholder's responsibilities and requirement. This approach takes a

holistic view of the organisation strategies and management information systems as it provides visibility across cross functional and business integrated activities. Furthermore, the IoMT Framework represents a good fit for the proposed new law as manufacturer will have the benefits of innovative design for products whilst still ensuring devices have the appropriate security and privacy requirements. Conceptually the IoMT Security and Privacy Framework was built on the inherent research principle which suggests that framing research activities to deal with the business needs gives credibility and relevance to the research.

References

1. Alsubaei F, Abuhussein A, Shiva S (2017) Security and privacy in the internet of medical things: taxonomy and risk assessment. In: 2017 IEEE 42nd conference on Local Computer Networks Workshops (LCN Workshops). IEEE, pp 112–120
2. Alsubaei F, Abuhussein A, Shiva S (2019) Ontology-based security recommendation for the internet of medical things. IEEE Access 7:48948–48960
3. Brenner J (2007) ISO 27001: risk management and compliance. Risk Manage 54(1):24
4. Data Governance Program. Available at: https://cio.ubc.ca/data-governance/data-governance-program. Accessed on: 24 July 2019
5. Farahat IS, Tolba AS, Elhoseny M, Eladrosy W (2018) A secure real-time internet of medical smart things (IOMST). Comput Electr Eng 72:455–467
6. Hevner AR, March ST, Park J, Ram S (2004, March) Design science in information systems research. MIS Q 28(1):75–105. https://doi.org/10.2307/25148625. Management Information Systems Research Center, University of Minnesota. https://www.jstor.org/stable/25148625
7. Jalali MS, Kaiser JP (2018) Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res 20(5):e10059
8. Osborne JW (ed) (2008) Best practices in quantitative methods. Sage, Los Angeles/London
9. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng 2017:9324035
10. Wolf M, Serpanos D (2017) Safety and security in cyber-physical systems and internet-of-things systems. Proc IEEE 106(1):9–20
11. Wrestling the data quality bull: using informatic IDQ so upstream business. Available at: http://sullexis.com/blog/wrestling-the-data-quality-bull-using-informatica-idq-so-upstream-business-users-can-grab-data-quality-by-the-horns-and-wrestle-it-to-submission/. Accessed on: 24 July 2019