Security Control Techniques: Cybersecurity & Medical Wearable Devices

Samuel Sambasivam
Samuel.Sambasivam@Woodbury.edu
Computer Science Data Analytics
Woodbury University
Burbank, CA 91504

Jeff Deal
Jeff@n6networks.com
N6Networks

Abstract

The Internet of things (IoT) has been a significant advancement in technology, advancing the modernization of repetitive tasks, streamlining data collection, and providing new ways to collect, interpret, and disseminate information. Numerous industries have benefited from advancements in IoT technology, including the healthcare industry. For example, medical IoT (MIoT) has deployed several devices, including internet-connected sleep apnea, blood pressure regulators, glucose monitoring, and mobile echocardiogram and heart rate monitors. The advancement in MoT devices has revolutionized medicine and the treatment of care. Both treatment facilities and patients perform a significant amount of care solutions from their homes, saving the patient time and money. However, the integration of technology to maintain potential life-sustaining functions within the patients comes with the challenge of ensuring that data integrity and patient safety are not compromised. This study leveraged a qualitative case study to understand the security controls and techniques cybersecurity professionals need to protect medical wearable devices. Participants were selected from a wide range of medical treatment facilities, including information system technicians, information system security officers, and chief information officers. The top three cybersecurity concerns identified by survey respondents are 1) IT professionals require a better understanding of how devices function – including criticality of health care task, authentication protocol, data transmission details, etc. 2) users/wearers lack a fundamental understanding of cybersecurity risks and available security functions/features 3) the cooperative role required by the device manufacturer, the medical treatment professional, IT professional, and users to properly secure MIoTs is not understood. Recommendations for cybersecurity professionals identify MIoT devices' standards based on identifying and prioritizing device function as a substantial factor for security risk assessments and ensuring devices deployed multi-factor authentication while maintaining a robust patching and security framework.

Keywords: Medical Wearable Devices, MIoT, IoT, Cybersecurity.

1. INTRODUCTION

Today's average citizen is more connected than ever (Pew Research Center, 2019). Technology is integrated into all aspects of our lives (Dutta, 2018). Data can now be requested from a simple voice query from smart home assistants such as Alexa, Contra, and Siri. The Internet of Things (IoT) area is evolving into multiple solutions from the corporate deployment to meet enterprise shortfalls to the integration into homes such as a doorbell, garage door openers, refrigerators, and camera systems. Martin (2019) reported that 69% of homes in the United States have at least

one smart device. Gartner (2014) identified that a significant majority of mobile device vendors had deployed wearable devices, which is a substantial increase from only two companies using wearable technology. The emerging threat towards healthcare and medical treatment facilities is on the rise. As IT systems become integrated into medical treatment solutions, the risk of data exposure, device compromise, and physical harm is significantly increased. The successful execution of malicious code is causing both a danger towards the integrated medical treatment facilities and the patient life-sustaining systems such as respirators, blood pressure, heart rate monitors, and insulin distributors.
Piwek et al. (2016) identified that one in six consumers utilizes a wearable device, including smartwatches, to collect health information.
Leveraging medical wearables or implantable devices, medical providers and treatment facilities can provide robust medical treatment options for patients worldwide (Li et al., 2017).

By interconnecting medical treatment facilities, information can be shared directly between the patient and provider, significantly reducing cost while maintaining high levels of care (McCaldin et al., 2016). In addition, specific devices such as insulin pumps, pacemakers, and defibrillators remotely monitored through an internet connection can provide patients with overall better quality of life (Mantas et al., 2016). The study aims to provide insight into how cybersecurity specialists implement different security controls to protect medical wearable devices. As the Internet provides numerous capabilities to organizations, healthcare is no stranger to advancing technology solutions. As a result, the term (IoT) has evolved and has created a sub-culture of devices identified as Medical IoT (MIoT). Devices that fall into the category of Medical IoT provide patients with remote monitoring of numerous services to include blood pressure, heart rate, echocardiogram (EKG), insulin deployment, and monitoring of oxygen levels. Medical IoT's benefits allow medical treatment facilities to deliver patient care remotely, reducing costs for patients. In addition, medical IoT devices can receive pre-programmed instruction sets to help patients in an emergency until they can be reached by a local healthcare professional.

2. RESEARCH PROBLEM

The problem addressed in this study was the security controls techniques cybersecurity specialists need to protect medical wearable devices have not been identified (McCaldin et al., 2016). The IoT industry has a $6.2 Trillion-dollar growth market, with a significant majority of devices identified as healthcare devices valued at 2.5 trillion (Brown, 2013). With numerous organizations entering the wearable technology area, one of the critical gap areas is device security and user privacy.

Lang (2018) identified that a considerable majority of healthcare treatment facilities could not manage the emerging threats related to enterprise IT solutions. Ransomware has become the weapon of choice when targeting healthcare organizations. Ragan (2016) noted that The Hollywood Presbyterian Medical Center (HPMC) targeted a ransomware attack that causes the organization to pay out $3.4 million in bitcoin to decrypt systems. With a significant number of healthcare organizations initially slowly integrating the cloud into the IT solution for healthcare operations, cloud service providers have seen a substantial increase in cloud utilization for healthcare services, including software deployment as a service (SaaS). Zhang and Ravishankar (2019) identified that organizations that leverage IaaS could increase productivity while reducing the on-premise footprint. While it was determined that the movement to cloud infrastructure was inevitable, there were several concerns regarding security (Zhou et al., 2010). Several challenges were discussed in the cloud on-demand model: security, performance, availability, and integration were rated the highest by survey participants. A significant number of MIoT devices leverage critical services such as patient monitoring of heart rate, oxygen levels, and echocardiogram data that have a necessary dependency on software that integrates with the patient and hardware devices. Proper monitoring of the patient's vitals can become compromised from the improper configuration of software, leading to the backdoor intrusion of devices (Miclăuș et al., 2019). Ransomware is a popular choice of cyber criminals against medical treatment facilities. Argaw et al. (2019) discussed that The Department of Justice identified over 4,000 ransomware attacks across medical treatment facilities across the United States. Identifying and discussing emerging threats towards medical treatment facilities and MIoT devices can help identify solutions that can bridge the gap in organization security posture and the overall cyber hygiene of medical treatment facilities. The "gap" can only be solved by increasing awareness as new challenges are presented daily. Increasing visibility in threats and implementing user best practices

play a critical role in integrating the defense-in-depth approach, including addressing hardware, software, procedures, and protocols to ensure patient safety.

3. POPULATION AND SAMPLE

This study's population included cybersecurity experts with roles and responsibilities for creating, implementing, enforcing, or improving the understanding of cybersecurity policies and related industry standards. In addition, the population included members from cybersecurity specialists from the International Information System Security Certification Consortium (ISC2), which provides for more than 150,000 certified members recognized globally for its advancement in the development of cyber and infrastructure security (ISC2, n.d.). The research study sample comprises 10 participants, identified as an appropriate sample by Creswell (1998). The target population is determined using several factors, including the scope of the research and the limitation of the researcher; however, Thomson (2010) discusses that the average sample size for qualitative research was 25 participants. Creswell (1998) identified a range of 20-30 participants. Morse and Field (1996) identified a range of 30-50 participants. The overall goal of leveraging recommended sample sizes is to ensure the researcher reaches saturation within the selected population.

Raw data were collected using the 13 interview questions:

1.What are the most significant cybersecurity threats to your medical treatment facility? 2.What is the most significant underlying issue with medical IoT devices?

3.What physical security measures do you implement to protect the current IT infrastructure?

4.What administrative security measures do you implement to protect the current IT infrastructure?

5.Who has the responsibility of securing medical wearable devices? Should the security role fall on the device manufacturer, the user, the medical treatment, the government, or a combination of all entities?

6.Do you think that Medical IoT devices should be identified in different priorities based on the function they serve?

7.With laws such as the General Data Protection Regulation in Europe, do you think there is a need for a legal framework to protect Medical IoT devices and the data generated?

8.In your opinion, does your organization place budget as a priority over security?

9.Do you subscribe to any security-related magazines, attend any trade shows, conferences, or are a part of any cybersecurity groups that discuss emerging threats?

10.If so, does it help you stay up to date on emerging threats and provide new methods of protection?

11. What direction should organizations take to protect medical wearable devices?

12. What are three items that should be a part of every cybersecurity specialist's playbook to protect medical wearable devices?

13. What can medical wearable device users protect themselves from potential data compromise or physical harm from a cybersecurity incident?

4. ANALYSIS OF DATA

In a study conducted by Williams and Woodward (2015), the researchers identified the increased connectivity and complexity medical wearable devices bring creates a complicated challenge. With the expansion and integration of technology and healthcare, the need to protect the information system from malicious attacks and the safety of both patients and data and physical harm. Moreover, the researchers discussed several areas of concern, including data storage and data transfer, which several participants also identified as a gap of security focus for medical device manufacturers.

Major Theme 1: Function

The theme regarding functions was a significant item of the discussion by all participants. Each participant identified that devices should be determined by the function they serve. The discussion primarily focused on identifying that cybersecurity specialists must identify how the devices function, including if the device supports life-sustaining functions such as heart rate, insulin control, blood pressure, and oxygen levels. Additionally, a function must also include how data is transmitted, received, and encrypted to and from the device, how the user authenticates with the device, and any additional operational safety functions or features. The implementation of system hardening is a common practice within the cybersecurity realm.

Hardening systems allow security practitioners to remove non-essential services such as open ports, protocols, services, and programs, reducing the entry point for attack. Devices that manage life-sustaining functions should implement multi-factor authentication, logging, and auditing. Multi-factor authentication (MFA) required the use of two or more verification factors to perform actions on a resource (Ometov

et al., 2018). Multi-factor authentication leverages several items including, something you know (i.e., security questions, passwords, and one time passcodes (OTP)), something you have (i.e., Tokens, OTP's sent over cellular or email messaging), and something you are (i.e., fingerprints, facial recognition, voice, retina) (Choi et al., 2017). Other MFA examples include Behavioral analysis such as gait when walking, location-based authentication leveraging IP address location. Risk-based authentication is another MFA method that leverages authentication attempts with behavioral analytics (Wiefling et al., 2019).

Authentication access is based on when a user tried to gain access, the device type, location services, and historical attempts to authenticate. Logging of the device's authentication attempts and transmission of data ensures that all information sent to and from the device is authorized and requires the user to present multiple authentication methods before executing commands on a device. Logging can provide a wide variety of metrics, including performance, behavioral and environmental data vital in supporting device function. Integrated with ML/AI devices can provide data sets allowing cybersecurity specialists to recognize anomalous activity and provide audit trails for all actions on the device (Muggler et al., 2017).

Major Theme 2: Users

The theme regarding users was discussed by 90% of the participants, with a significant majority of discussion surrounding the user's knowledge base and responsibility while using medical wearable devices. The participants describe users in both the medical treatment facility who are intermediate or 3rd party users of the device maintain the CIA triad of confidentially, integrity, and availability. Participants discussed that users often lacked training on operating the device, unaware of the security functions or features, and are unaware of the risk that the user's mismanagement of devices brings the enterprise IT infrastructure. Users are a significant part of an organization's cybersecurity posture. Cain et al. (2018) discussed that end users are often identified as the weakest point as 95% of attacks are aimed at users. Kweon et al. (2019) further recognized a direct relation between leveraging cybersecurity training and reducing cybersecurity incidents.

Major Theme 3: All Entities

The theme regarding all entities was discussed by 9 out of 10 participants representing the need for a robust cybersecurity approach to protecting medical wearable devices. Participants stressed the need for multiple entities to be involved in the cybersecurity process. All entities include the inception of the device developer. The doctors/nurses present with the device are recommended as a treatment solution, cybersecurity specialists who managed MIoT devices on the network, and the end-users who leveraged the device as treatment solutions. The device manufacture should ensure not only ensure the physical security of the devices. It should also perform code validation of the software and firmware that the device will use to control or monitor the patient's bio-health systems. Doctors, nurses, and medical staff need to understand how the device supports the patient's health but must be aware of the potential side effects of cybersecurity vulnerabilities and the risks of threats related to MIoT.

Cybersecurity specialists that work within medical treatment facilities must also understand risk by correctly identifying which devices are on the network, the device classification/function, and the different threats each type of device presents to the infrastructure. Users must also understand the risk involved with device usage, data encryption, transport security, and the safety function to ensure the device operates at peak efficiency without compromising the device, user, or treatment facility. Potential hackers can compromise devices that do not implement robust security controls. Unencrypted medical data is a data-rich target for potential hackers. Security professionals have seen a spike in cyberattacks towards hospitals as security and encryption are often misconfigured or not implemented. The Catawba Valley Medical Center was a recent victim of a cyberattack exposing over 20,000 patient records compromised through a phishing attempt that compromised three employee's accounts. Hackers were able to access protected health information that, if encrypted, could potentially reduce the likelihood of exposed personal health data.

Major Theme 4: Legal Framework

All participants identified that some established frameworks help protect data in the medical Field, including HIPPA and PII laws, but the gap was in protecting MIoT devices. Users are more invested in understanding what data is being collected from the end devices and how the information is being used. The European Union has taken legal action to hold the organization accountable for the data collection process, transmission, collection, and usage of end-users data. Participants stressed that the United States was behind in establishing a national legal framework

regarding the use of user data. California has taken an individual step forward in implementing a legal framework in the establishment of SB 327, which required device manufacturers to ensure devices are equipped with reasonable security features, including the protection of the data collected, contained, or transmitted. While one state strives to protect data, device users may become unprotected if the user data is generated outside of California, as SB-327 only identifies protections for California residency (Eagan, 2020).

5. CONCLUSION

The study on the security control techniques cybersecurity experts needs to protect the medical wearable device identified the functional areas to address when integrating MIoT devices within a medical treatment facility. The literature review identified the massive integration of IoT devices across all platforms. The MIoT device adoption provides new methods for delivering medical care in remote and unique medical treatment scenarios. Cost savings, reduced visits, and prioritization of care treatment are all benefits of MIoT adoption. The integration of technology supporting life-sustaining functions presented several challenges to cyber professionals, including physical safety and the potential loss of life from a compromised device and information security for data transmitted to and from the device (Bonderud, 2019). Each case enforces the need to support a robust cybersecurity solution to enforce the protection of medical wearable devices and ensure both the safety from physical harm and privacy of patient data. As the adoption of wearable devices use increases cybersecurity professionals can leverage the four themes identified as security foundations for the establishment of a security program and framework when implementing MIoT devices within the organization. The identification of security shortfalls identified in this study can act as the launch point in the discussion of controls needed in the establishment of cyber hygiene and cyber posture. Stakeholders play a significant role in the deployment of organization security as funding and executive buy-in are often controlled by shareholders/stakeholders. Cyber professionals and senior leadership can leverage the information and security shortfalls understanding the risk associated with the importance of user awareness, and the role each entity plays with the implementation and maintenance of integrated MIoT devices.

6. FUTURE RESEARCH

The study was intended to determine the security control techniques cybersecurity specialists need to protect medical wearable devices that expand upon what is known within the current literature and identify opportunities from experienced participants. The participants for this study were IT professionals supporting the medical IT infrastructure. The insights and knowledge of IT professionals who participated in this research study provided clear details on the different strategies needed to protect medical wearable devices. The research study provided valuable information and data, which identified recommendations for further research.

Recommendation 1 is the need for data protection concerning big data generated through wearable devices. Medical wearable devices can generate vast amounts of data to find underlying solutions providing more robust healthcare solutions through data collection and processing. Data generated by medical wearable devices can become a gold mine for insurance companies. Olson (2014) discusses that a significant amount of insurance data is driven by behavior. Numerous insurers in multiple arenas use data points to shape rates based on behavior-driven data. Medical wearable devices could give insurance companies near-real-time data with reasonable latency tolerances to support their users' habitual actions. This research effort would benefit from identifying the best tactics for supporting privacy concerns related to wearable devices and further investigating the relationship between healthcare and insurance providers who collect and use the data to help the device users (Leedy & Ormrod, 2010).

Recommendation 2 is additional research is needed concerning medical wearable device type security. Medical wearable devices vary in different types based on different functions. Devices that are passive such as heart rate monitors and oxygen level monitors, may need more or fewer security functions than devices that support life-sustaining MIoT functions such as blood pressure monitors, echocardiograms, and pacemakers. More research is needed with the underlying framework or legislation on the proper deployment and management of Medical IoT devices. This research effort would benefit from the comparison approach of security between passive and active MIoT devices as there is a lack of knowledge of security vulnerabilities based on active and passive MIoT devices. (Leedy & Ormrod, 2010).

7. REFERENCES

Argaw, S. T., Bempong, N.-E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Medical Informatics and Decision Making*, *19*(1). https://doi.org/10.1186/s12911-018-0724-5

Bonderud, D. (2019, June 19). IoT Security and the Enterprise: A Practical Primer. Security Intelligence; Security Intelligence. https://securityintelligence.com/articles/iot-security-and-the-enterprise-a-practical-primer/

Brown, A. (2013). *M2M Revenues by Industry Vertical*. Strategyanalytics.com. https://www.strategyanalytics.com/access-services/enterprise/iot/reports/report-detail/m2m-revenue-industry-vertical

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Choi, Y., Lee, Y., Moon, J., & Won, D. (2017). Security enhanced multi-factor biometric authentication scheme using bio-hash function. *PLOS ONE*, *12*(5), e0176250. https://doi.org/10.1371/journal.pone.0176250

Creswell, J. (1998). *Qualitative inquiry and research design: Choosing among five traditions* (p. 64). Sage.

Dutta, P. (2018). *How Technology Is Influencing Humanity In Daily Life*. Thriveglobal.com. https://thriveglobal.com/stories/how-technology-is-influencing-humanity-in-daily-life/

Eagan, C. (2020, January 9). *California's IoT cybersecurity bill: What it gets right and wrong*. Help Net Security. https://www.helpnetsecurity.com/2020/01/09/californias-iot-cybersecurity-bill/

Gartner. (2014). *Gartner Says Worldwide Smartwatch and Wristband Market Is Poised for Take Off*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2014-09-17-gartner-says-worldwide-smartwatch-and-wristband-market-is-poised-for-take-off

ISC2. (n.d.). *Why Join (ISC)² | Benefits of Membership*. Www.isc2.org. Retrieved January 26, 2021, from https://www.isc2.org/Benefits-of-Membership#

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09977-z

Lang, U. (2018). Securing Complex Cyber-Physical Medical Device Landscapes. *Information System Security Association*, *16*(4). https://objectsecurity.com/tmp/2018.04.ISSAJournal.UlrichLang.MedicalDeviceSecurity-article.pdf

Leedy, P. D., & Ormrod, J. E. (2010). Practical research.

Li, C.-T., Wu, T.-Y., Chen, C.-L., Lee, C.-C., & Chen, C.-M. (2017). An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System. *Sensors*, *17*(7), 1482. https://doi.org/10.3390/s17071482

Mantas, J., Hasman, A., Gallos, P., Kolokathi, A., & Househ, M. (2016). Unifying the applications and foundations of biomedical and health informatics. *Technology and Informatics*.

Martin, C. (2019). *Smart Home Technology Hits 69% Penetration in U.S.* Www.mediapost.com. https://www.mediapost.com/publications/article/341320/smart-home-technology-hits-69-penetration-in-us.html

McCaldin, D., Wang, K., Schreier, G., Lovell, N. H., Marschollek, M., Redmond, S. J., & Schukat, M. (2016). Unintended Consequences of Wearable Sensor Use in Healthcare. *Yearbook of Medical Informatics*, *25*(01), 73–86. https://doi.org/10.15265/iy-2016-025

Miclăuș, T., Valla, V., Koukoura, A., Nielsen, A., Dahlerup, B., Tsianos, G., & Vassiliadis, E. (2019). Impact of Design on Medical Device Safety. *Therapeutic Innovation & Regulatory Science*. https://doi.org/10.1007/s43441-019-00022-4

Morse, J. M., & Field, P. A. (1996). An overview of qualitative methods. *Nursing Research*, 18–34. https://doi.org/10.1007/978-1-4899-4471-9_2

Muggler, M., Eshwarappa, R., & Cankaya, E. C. (2017). Cybersecurity Management Through Logging Analytics. *Advances in Intelligent Systems and Computing*, 3–15. https://doi.org/10.1007/978-3-319-60585-2_1

Olson, P. (2014). Wearable Tech Is Plugging Into Health Insurance. Forbes. http://www.forbes.com/sites/parmyolson/20

14/06/19/wearable-tech-health-insurance/#16d50cff5ba1.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Pew Research Center. (2019, October 28). *The Internet will continue to make life better*. Pew Research Center: Internet, Science & Tech; Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/10/28/4-the-internet-will-continue-to-make-life-better/

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The Rise of Consumer Health Wearables: Promises and Barriers. *PLOS Medicine*, *13*(2), e1001953. https://doi.org/10.1371/journal.pmed.1001953

Ragan, S. (2016, February 14). *Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers*. CSO Online. http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-

Thomson, S. (2010). Sample Size and Grounded Theory. *Journal of Administration and Governance*, *5*(1), 45–52.

Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2019). Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. *ICT Systems Security and Privacy Protection*, 134–148. https://doi.org/10.1007/978-3-030-22312-0_10

Williams, P., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305. https://doi.org/10.2147/mder.s50048

Zhang, G., & Ravishankar, M. (2019). Exploring vendor capabilities in the cloud environment: A case study of Alibaba Cloud Computing. *Information & Management*, *56*(3), 343–355. https://doi.org/10.1016/j.im.2018.07.008

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *Sixth International Conference on Semantics, Knowledge, and Grids*, *IEEE*(), 105–112. https://doi.org/10.1109/skg.