APPLYING THE HEALTH BELIEF MODEL TO CARDIAC IMPLANTED MEDICAL DEVICE PATIENTS

George W. Jackson[1] and Shawon Rahman[2]

[1]College of Business and Technology, Capella University, Minneapolis, USA
[2]Professor, Dept.of Computer Science & Engineering, University of Hawaii-Hilo, 200W.KawiliStreet, Hilo, HI96720, USA

ABSTRACT

Wireless Implanted Medical Devices (WIMD) are helping millions of users experience a better quality of life. Because of their many benefits, these devices are experiencing dramatic growth in usage, application, and complexity. However, this rapid growth has precipitated an equally rapid growth of cybersecurity risks and threats. While it is apparent from the literature WIMD cybersecurity is a shared responsibility among manufacturers, healthcare providers, and patients; what explained what role patients should play in WIMD cybersecurity and how patients should be empowered to assume this role. The health belief model (HBM) was applied as the theoretical framework for a multiple case study which examined the question: How are the cybersecurity risks and threats related to wireless implanted medical devices being communicated to patients who have or will have these devices implanted in their bodies? The subjects of this multiple case study were sixteen cardiac device specialists in the U.S., each possessing at least one year of experience working directly with cardiac implanted medical device (CIMD) patients, who actively used cardiac device home monitoring systems. The HBM provides a systematic framework suitable for the proposed research. Because of its six-decade history of validity and its extraordinary versatility, the health belief model, more efficiently than any other model considered, provides a context for understanding and interpreting the results of this study. Thus, the theoretical contribution of this research is to apply the HBM in a setting where it has never been applied before, WIMD patient cybersecurity awareness. This analysis (using a multiple case study) will demonstrate how the HBM can assist the health practitioners, regulators, manufacturers, security practitioners, and the research community in better understanding the factors, which support WIMD patient cybersecurity awareness and subsequent adherence to cybersecurity best practices.

KEYWORDS

Health Belief Model, Healthcare Cybersecurity, Cardiac Implanted Device, Wireless Implanted Medical Devices, WIMD, WIMD cybersecurity,

1. INTRODUCTION

There are several parallels between information security and preventive medicine [1, 2, 3]. In preventive medicine, there is the need to avoid risky behavior; likewise, in information security, there is also a need to avoid risky behavior. In information security, there is the need to initiate and maintain proactive measures (e.g., software patching and updating) and in preventive medicine, there is a need to engage in measures such as disease immunization and so on. As the proposed research is solidly in the field of healthcare, a 64-year-old, universally accepted, healthcare-derived, healthcare-based theory, especially one proven to apply to information security, was a natural fit. The HBM is also a viable research framework, as well as a useful tool for analysis and a readily accessible context for the interpretation of research results. The health belief model has enjoyed a range of applications inside and outside of the field of healthcare. For

example, [4] found the HBM to be a suitable model for assessing user perception in the Financial Services industry.

HBM begins with perception, and the assessment of perception is the backbone of this research study. HBM seeks to understand the patient's perception of risks to their health (denoted as perceived susceptibility to disease and perceived severity of disease). After this, HBM examines modifying factors such as age, sex, ethnicity, personality, culture, socioeconomics, knowledge, self-efficacy, and cues to action. These modifying factors are an integral part of the WIMD patient's lived experience. The final HBM outcome is an assessment of an individual's likelihood of acting on his or her behalf. An objective of the proposed research is to form an evaluation of how these factors are brought to bear on a WIMD patient's experience. Health behavior models, such as the HBM can be useful for increasing information security awareness [5]. In HBM, all the perception and modifying factors funnel themselves into a prediction of the likelihood of taking action.

The ability to anticipate a WIMD patient's likelihood of adhering to cybersecurity best practices is a desired outcome of the proposed research. All the same, criticism has been leveled that the health belief model fails to address the importance of intentions or the influence the approval or disapproval of others might play as far as intentions and behavior [6]. It is also interesting to note in recent years there has been the emergence of a security belief model (SBM) based upon the health belief model [1], as a way of addressing intentionality.

Additionally, [7] cited [8] in suggesting the theory of planned behavior (TPB) might be superior to the HBM in assessing relationships between the attitude, intention, and action for the sake of information security policymaking in an organizational setting. Indeed, this may be exactly true in a purely corporate environment focused upon policy-making and compliance. However, placing these perceived shortcomings aside, for this study on WIMD patient cybersecurity awareness, the HBM provides an end-to-end, systematic framework suitable for the proposed research. Because of its six-decade history of validity and its extraordinary versatility, the health belief model, more efficiently than any other model considered, provides a context for understanding and interpreting the results of this study.

Thus, the theoretical contribution of this research is to apply the HBM in a setting where it has never been applied before, WIMD patient cybersecurity awareness. This analysis (using a multiple case study) will demonstrate how the HBM can assist the health practitioners, regulators, manufacturers, security practitioners, and the research community in better understanding the factors, which support WIMD patient cybersecurity awareness and subsequent adherence to cybersecurity best practices.

2. LITERATURE REVIEW

Several parallels between information security and preventive medicine were discussed in [1] as well as [2] and [3]. In preventive medicine, there is the need to avoid risky behavior; likewise, in information security [38], there is also a need to avoid risky behavior. In information security, there is the need to initiate and maintain proactive measures (e.g., software patching and updating) and in preventive medicine, there is a need to engage in measures such as disease immunization and so on. As the proposed research is solidly in the field of healthcare, a 64- year-old, universally accepted, healthcare-derived, healthcare-based theory, especially one proven to apply to information security, was a natural fit. The HBM is also a viable research framework, as well as a useful tool for analysis and a readily accessible context for the interpretation of research results. The health belief model has enjoyed a range of applications inside and outside of the field

of healthcare. For example, [4] found the HBM to be a suitable model for assessing user perception in the Financial Services industry.

HBM begins with perception, and the assessment of perception is the backbone of this research study. HBM seeks to understand the patient's perception of risks to their health (denoted as perceived susceptibility to disease and perceived severity of disease) [39]. After this, HBM examines modifying factors such as age, sex, ethnicity, personality, culture, socioeconomics, knowledge, self-efficacy, and cues to action. These modifying factors are an integral part of the WIMD patient's lived experience. The final HBM outcome is an assessment of an individual's likelihood of acting on his or her behalf.

An objective of the proposed research is to form an evaluation of how these factors are brought to bear on a WIMD patient's experience. The ability to anticipate a WIMD patient's likelihood of adhering to cybersecurity best practices is a desired outcome of the proposed research. The HBM provides an end-to-end, systematic framework suitable for the proposed research. Because of its six-decade history of validity and its extraordinary versatility, the health belief model, more efficiently than any other model considered, provides a context for understanding and interpreting the results of this study.

Thus, the theoretical contribution of this research is to apply the HBM in a setting where it has never been applied before, WIMD patient cybersecurity awareness. This analysis (using a multiple case study) will demonstrate how the HBM can assist the health practitioners, regulators, manufacturers, security practitioners, and the research community in better understanding the factors, which support WIMD patient cybersecurity awareness and subsequent adherence to cybersecurity best practices.

3. APPLYING THE HEALTH BELIEF MODEL TO THE STUDY

These study's findings were examined in the light of the theoretical framework of the health belief model (HBM). The HBM is a behavioral model that seeks to predict the likelihood thata patient will be motivated to take actions on their behalf in a preventative healthcare situation. This theoretical framework fits well with the study as an essential goal of discovering how WIMD risks and threats are communicated to patients was to provide clues as to how patient's cybersecurity perceptions are being formed and to what effect. The fundamental HBM components of perceived susceptibility and severity, perceived threat, perceived benefits versus perceived barriers, and perceived self-efficacy are combined with modifying factors (such as demographics) as well as cues to action, to determine the likelihood a patient will take preventive measures on their behalf. The constructs of the HBM theoretical framework and their definitions have been aligned with the study's five themes as a way of engaging a more rigorous interpretation of the study's findings. An overview is presented in Table 1, followed by a detailed discussion. Additionally, these findings are compared with past and current WIMD cybersecurity literature. Convergences and divergences between the study and extant literature are noted.

3.1. Perceived Susceptibility and the Impact of Cyber Influence

In the health belief model, perceptions give rise to individual beliefs, and individual beliefs are the primary determinants of individual behavior. The HBM, as a predictive model, recognizes the need for a patient to experience a personal connection to the phenomenon of care to become motivated enough to change or assume a new behavior. This underscores the importance of considering all the factors that influence a WIMD patient's perception of the cybersecurity risks and threats to their health. A patient must experience susceptibility as being real and being

personal. In the tidal wave of cybersecurity data and information, it is those centers of influence that reach and resonate most with a patient that will impact that patient's understanding of their susceptibility or vulnerability to harm.

Table 1. Alignment of Theoretical Framework with Research Findings

Health Belief Model Construct	Construct Definition	Associated Research Finding
Perceived Susceptibility	Perceived Susceptibility are beliefs a patient has about the likelihood of their experiencing a disease or harmful event (Hayden, 2013).	Multiple Factors influence Cybersecurity
Perceived Severity	Perceived Severity are beliefs a patient has about the severity of consequences from not adopting a behavior (Hayden, 2013).	Impartial Data required for accurate Risk Analysis
Perceived Threat	Perceived Threat are beliefs a patient has about severity and susceptibility to a harmful event combined. (Hayden, 2013).	Risk communications must move towards proactivity
Perceived Benefits	Perceived Benefits are beliefs a patient has about the positive impact of adopting a health behavior (Hayden, 2013).	Cybersecurity Awareness Collaborative Effort
Perceived Barriers	Perceived Barriers are beliefs a patient has about the obstacles to adopting a health behavior (Hayden, 2013).	Cybersecurity Awareness Collaborative Effort
Cues to Action	Cues to Action are internal or external factors, which prompt or influence a preventive health behavior (Hayden, 2013).	Education required for Patient, Providers, and Industry
Perceived Self-efficacy	Perceived Self-efficacy are beliefs a patient has about their ability to perform a given health behavior (Hayden, 2013).	Education required for Patient, Providers, and Industry

Reflection on Previous Literature. The importance of patient awareness and engagement in medical device cybersecurity was referenced in [9, 10, 11, 12, 13, 14, 15, and 16] While wireless implanted medical devices share the same vulnerabilities as any networked device [17] what makes WIMD cybersecurity unique is that security enhancements to an implanted device, as we saw in this study, might require surgery [9]. Because the patient and the device are physically connected, the patient should be made aware of vulnerabilities in their device, represented by the construct of perceived susceptibility.

3.2. Perceived Severity and Risk Analysis

Added to their susceptibility to harm patients need to understand the consequences of a harmful event and the severity of its impact. Perceived severity is a significant element of risk identification, assessment, and analysis. Today this crucial factor rests in the hands of the device industry, healthcare providers, and the media. Nevertheless, careful risk analysis focused on the direct, impact to the patient--as suggested by the HBM--would uncover both physical

consequences (death, disability, pain, and the like) and social consequences (inability to work, interruption of routine, impact on relationships with family, friend, and other support groups). A stream of reliable data, from impartial sources, analyzed in an unbiased manner would help to create a holistic perception of severity for the patient.

Reflection on Previous Literature. According to [18] it has been estimated the security standards surrounding medical devices are nearly a decade behind modern security standards. What is more, [19] stated the results of a cybersecurity attack against a healthcare organization could be anywhere from being minor to being fatal. Also keeping in mind, 94% of healthcare organizations reported being victims of a cyber-attack [20]. Every WIMD patient, regardless of device, must rely on their device manufacturer and their healthcare provider to protect them, [21 and 22]. While it may be difficult to launch a cyber-attack against an individual active medical device, it has been proven to be far from impossible, [23, 24, 25, 26, 13, 27]. What is more, both the healthcare and the medical device industry's information security substructures are woefully ill-prepared to thwart the growing cybersecurity threat [26, 21, 22, 28, 41]. Last, the entire wireless implanted medical device cybersecurity ecosystem is profoundly at risk. [29, 13, 30, 22, 40, 44, 45].

Because medical devices have become increasingly interconnected, there no longer must be a direct attack, on a specific device, for a WIMD patient to potentially experience a severe impact [9, 11, 12, 28, 42]. One cannot truly convey the severity of risk without discussing the vulnerabilities present throughout the entire system in which that device is connected. Which admittedly, is a difficult conversation; however, failing to do so prevents patients from seeing the complete picture of risks and severity.

3.3. Perceived Threat and Cybersecurity Risk Communications

Perceived Threat is a crucial motivator in the HBM. In the HBM framework, the perceived threat is comprised of perceived susceptibility combined with perceived severity. There via the HBM cybersecurity threats are a function of the patient's perceived susceptibility combined with the patient's perceived severity. This the HBM would prescribe that patient cybersecurity threat communications should, at a minimum, include full disclosure of cybersecurity vulnerabilities (perceived susceptibility) as well as a full disclosure of the possible physical and social impacts to the patient (perceived severity).

Reflection on Previous Literature. As noted earlier, wireless implanted medical devices help millions of patients, in a variety of disease areas, experience a higher quality of life [31, 16]. Due to the undeniable benefits gained from these devices, wireless implanted medical devices are experiencing dramatic growth in usage, application, and complexity [11, 12, 30]. Nevertheless, this rapid growth has brought a proliferation of cybersecurity threats [28, 43]. For example, [31] provided a detailed description of lethal attacks, which could be directed specifically at a cardiac implanted medical device. Previous research substantiated that cardiac implanted medical devices could be remotely compromised in a way that can cause harm to the device and the patient [32], [32], and [34]. From an HBM perspective, there is an obligation, from a purely ethical standpoint, to outline known cybersecurity threats to WIMD patients to support perceived susceptibility as well as perceived severity.

3.4. Perceived Benefits, Perceived Barriers, and Collaboration

Per the HBM, perceived benefits are the patient's beliefs about positive results that will come about because of their taking action. The desired action to be taken as far as the patient's role in

WIMD cybersecurity is for the patient to learn enough about the device in their bodies, and its interaction with other networked devices to be able to engage in meaningful decision making about issues related to their health and wellbeing (including cybersecurity issues). The next desired action for the patient is to remain an active participant in their medical care and device management [45] (including those aspects related to device cybersecurity).

While there are barriers to this optimal patient position and outlook, it seems fair to suggest that healthcare providers and device manufacturers should be significant proponents of removing those barriers—in a perfect world. The study demonstrates several levels of communication must take place between industry representatives, healthcare providers, and patients to allow patients to overcome barriers and realize the perceived benefits of taking action on their behalf to improve their knowledge of cybersecurity and the risks and threat involved with their device.

Reflection on Previous Literature, from the standpoint of the HBM theory, it is essential to view perceived benefits and perceived barriers from the patient's perspective. As previous academic and non-academic literature was extremely vague about the patient's role in WIMD cybersecurity, there is little to be found regarding patient's perceptions of barriers or benefits in previous literature.

3.5. Perceived Self-Efficacy and Cybersecurity Awareness

The HBM constructs of perceived self-efficacy, cues to action, and the modifying factor of patient demographics (and socials factors) are grouped into one category for this portion of the discussion as all these factors can be addressed through a combination of education and collaboration. The results of the study made it clear there are significant gaps in cybersecurity knowledge and information for patients and healthcare providers. A robust collaboration among all parties is needed to develop a pervasive, expansive, and proactive cybersecurity awareness program. A cybersecurity awareness program much like the Center of Excellence described by Participant 02 in the second study. Such a center of excellence, or a similar approach, addresses demographic issues, the primary one, in this case, being age, social factors such as computer literacy and acceptance of technology, socioeconomic problems such as illiteracy and works to foster self-efficacy on the part of the patient.

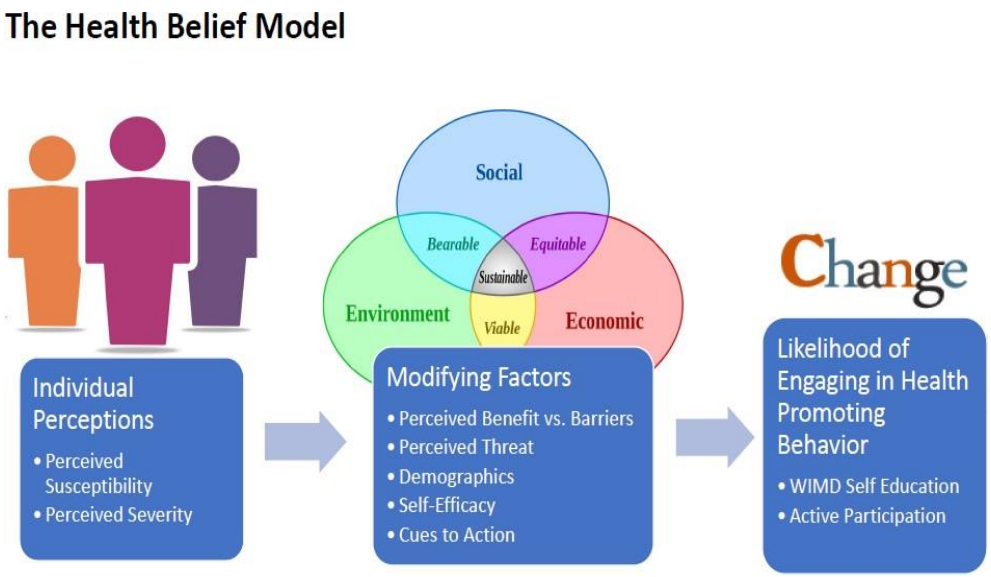

Figure1.The Health Belief Model.

4. CONCLUSIONS

After considering the study's results, in the light of the health belief model as well as the past literature, it is possible to lay bare additional interpretations of the data analysis findings. For example, to better address a patient's perception of threat (perceived susceptibility plus perceived severity) there is a strong need for on-going cybersecurity research that provides trustworthy and unbiased information to patients, providers, and the industry. Reliable research is required to support realistic perceptions of a patient's susceptibility to harm and the severity of the harm they might face from a cybersecurity threat.

Several participants observed that patient comprehension and ability to cope with the responsibilities and challenges of having wireless implanted medical devices would vastly improve if patient education and cybersecurity awareness began as early as possible, preferably before surgery. Increasing a patient's ability to comprehend and cope adds to their perceived self-efficacy, which directly contributes to the likelihood, per the health belief model, of a patient engaging in health-promoting behavior. For this study, those health-promoting behaviors are learning as much as possible about their device and remaining active and engaged participant in all aspects of their treatment.

By transitioning from reactive to proactive cybersecurity risk and threat communications healthcare providers, in combination with the medical device industry, will be able to provide WIMD patients with better and timelier cues to action. The HBM demonstrates (in concert with a perceived threat, self-efficacy, and perceived benefits versus perceived barriers) that cues to action provide the spark, which ignites positive health behaviors.

Finally, in helping patients see that the benefits of taking action outweigh the discomforts of overcoming physical, mental, or socioeconomic obstacles, healthcare providers, with the support of the industry, must be ready to assume a multi-faceted, iterative approach to patient communications and patient education to address a complex subject like patient cybersecurity awareness. Keeping in mind, healthcare organizations and their staff also require ongoing cybersecurity awareness training and education.

REFERENCES

[1] Lee, S. Hyun. & Kim Mi Na, (2008) "This is my paper", ABC Transactions on ECE, Vol. 10,No. 5, pp120-122.

[2] Gizem, Aksahya & Ayese, Ozcan (2009) Communications & Networks, Network Books, ABC Publishers.

[3] Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining users' security behaviors with the security belief model. Journal of Organizational and End User Computing, 26(3), 23-46.

[4] Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

[5] Jung, E. E., Ho, E. Y., Chung, H., & Sinclair, M. (2015). Perceived risk and self-efficacy regarding internet security in a marginalized community. Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, ACM, 1085-1090.

[6] Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology-mediated financial transactions. International Journal of Human-Computer Studies, 72(2), 154-168.

[7] Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). The effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, 5(26), 10862-10868.

[8] Marton, C., & Chun, W. C. (2012). A review of theoretical models of health information seeking on the web. Journal of Documentation, 68(3), 330-352.
[9] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106-125.
[10] Armitage, C. J., & Conner, M. (2000). Social cognition models and health behaviour: A structured review. Psychology and health, 15(2), 173-189.
[11] Camara, C., Peris-Lopez, P., & Tapiador, J.E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 55, 272-289.
[12] Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., & Maisel, W. H. (2010). Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 917-926.
[13] Fu, K. (2009). Inside risks: Reducing risks of implantable medical devices. Communications of the ACM, 52(6), 25-27.
[14] Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. Communications of the ACM, 56(10), 35-37
[15] Kotz, D. (2011). A threat taxonomy for mHealth privacy. Proceedings of Third International Conference on Communication Systems and Network (COMSNETS), 1-6.
[16] Leavitt, N. (2010). Researchers fight to keep implanted medical devices safe from hackers. Computer, 43(8), 11-14.
[17] Ray, A., Jones, P., & Zhang, Y. (2013). Medical device security-A new frontier. Biomedical Instrumentation & Technology, 47(1), 72-72.
[18] Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security Challenges for Medical Devices. Communications of the ACM, 58(4), 74-82.
[19] Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research, 8, 305–316.
[20] Middaugh, D. J. (2016). Do security flaws put your patients' health at risk? MedSurg Nursing, 25(2), 131-133.
[21] Boulos, P., Sargolzaei, A., Ziaei, A., & Sargolzaei, S. (2016). Pacemakers: A Survey on Development History, Cyber-Security Threats, and Countermeasures.
[22] Perakslis, E. D. (2014). Cybersecurity in health care. New England Journal of Medicine, 371(5), 395-397.
[23] Lyon, D. (2016). Making Trade-Offs for Safe, Effective, and Secure Patient Care. Journal of Diabetes Science and Technology,
[24] Sansurooah, K. (2015). Security risks of medical devices in wireless environments.
[25] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. International Journal of Internet and management, 6(4), 279-314.
[26] Armstrong, D. G., Kleidermacher, D. N., Klonoff, D. C., & Slepian, M. J. (2015). Cyber security regulation of wireless devices for performance and assurance in the age of “medjacking”. Journal of Diabetes Science and Technology, 1-4.
[27] Garfinkel, S. L. (2012). The cybersecurity risk. Communications of the ACM, 55(6), 29-32. [28] Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. Journal of diabetes science and technology.
[29] Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014). SoK: Security and privacy in implantable medical devices and body area networks. Proceedings of IEEE Security and Privacy 2014 Symposium, 524-539.
[30] Wirth, A. (2011). Cybercrimes pose growing threat to medical devices. Biomedical Instrumentation & Technology, 45(1), 26-34.
[31] Hansen, J. A., & Hansen, N. M. (2010). A taxonomy of vulnerabilities in implantable medical devices. In Proceedings of the Second Annual Workshop On Security and Privacy in Medical and Home-Care Systems, 13-20/
[32] Murphy, S. (2015). Is cyber security possible in healthcare? National Cybersecurity Institute Journal,1(3)49-63.

[33] Gupta, S. (2012). Implantable Medical Devices-Cyber Risks and Mitigation Approaches. In Proceedings of the Cybersecurity in Cyber-Physical Workshop, The National Institute of Standards and Technology (NIST), US.
[34] Ellouze, N., Rekhis, S., Boudriga, N., & Allouche, M. (2017). Cardiac Implantable Medical Devices forensics: Postmortem analysis of lethal attacks scenarios. Digital Investigation, 21, 11- 30.
[35] Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008). Security and privacy for implantable medical devices. IEEE pervasive computing, 7(1), 30-39.
[36] Burleson, W., Clark, S. S., Ransford, B., & Fu, K. (2012, June). Design challenges for secure implantable medical devices. In Proceedings of the 49th Annual Design Automation Conference (pp. 12-17). ACM.
[37] Rostami, M., Burleson, W., Koushanfar, F., & Juels, A. (2013, May). Balancing security and utility in medical devices? In Proceedings of the 50th Annual Design Automation Conference (p. 13). ACM.
[38] Faizi, Salman and Rahman, Shawon;" Securing Cloud Computing Through IT Governance"; International Journal of Information Technology in Industry (ITII), vol. 7, no.1, 2019, Pages: 1-14
[39] Jackson, George and Rahman, Shawon; "Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications related to the Medical Internet of Things (MIoT)", International Journal of Network Security & Its Applications (IJNSA), Vol. 11, No.4, July 2019.
[40] Loukaka, Alain and Rahman, Shawon; "Discovering New Cyber Protection Approaches From a Security Professional Prospective"; International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.4, July 2017
[41] Al-Mamun, Abdullah, Rahman, Shawon and et al;" Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte "; International Journal of Computer Networks & Communications (IJCNC), Vol.9, No.2, March 2017
[42] Opala, Omondi John; Rahman, Shawon; and Alelaiwi, Abdulhameed; "The Influence of Information Security on the Adoption of Cloud computing: An Exploratory Analysis", International Journal of Computer Networks & Communications (IJCNC), Vol.7, No.4, July 2015
[43] Faizi, Salman and Rahman, Shawon; "Secured Cloud for Enterprise Computing"; 34th International Conference on Computers and Their Applications (CATA-2019), March 18-20, 2019, Waikiki Beach Marriott Resort & Spa, Honolulu, Hawaii, USA
[44] Faizi, Salman and Rahman, Shawon; "Choosing the Best-fit Lifecycle Framework while Addressing Functionality and Security Issues"; 34th International Conference on Computers and Their Applications (CATA-2019), March 18-20, 2019, Waikiki Beach Marriott Resort & Spa, Honolulu, Hawaii, USA
[45] Schneider, Marvin and Rahman, Shawon "Protection Motivation Theory Factors that Influence Undergraduates to Adopt Smartphone Security Measures "; International Journal of Information Technology in Industry (ITII), Vol 9, No 1 (2021)

AUTHORS

Dr. George W. Jackson, Jr. has earned a Ph.D. in Information Technology, Information Assurance, and Cybersecurity degree from Capella University. He has nearly 30 years of experience in Information Technology, Information Security, and IT Project Management. A seasoned business and technology expert possessing an MBA and IT Management and professional certifications in Project Management, Information Security, and Healthcare Information Security and Privacy.

Dr. Shawon S. M. Rahman is a Professor of Computer Science at the University of Hawaii-Hilo and a part-time faculty of Information Technology, Information Assurance and Security Program at the Capella University. Dr. Rahman's research interests include software engineering education, information assurance and security, digital forensics, web accessibility, cloud computing, and software testing and quality assurance. He has published over 125 peer reviewed articles in various international journals, conferences, and books. He is an active member of many professional organizations including IEEE, ACM, ASEE, ASQ, and UPE.