Healthcare in the Balance: A Consequence of Cybersecurity

Susan Helser, Ph.D
Business Information Systems
Central Michigan University
Mount Pleasant, USA
helse1s@cmich.edu

Abstract—The mandate for cybersecurity crosses disciplines. The deficit in the number of cybersecurity professionals required to fill current and future positions represents a growing challenge. Cybersecurity readiness presents significant ever-changing issues with possible long-term or perhaps life-threatening consequences. Cybersecurity experts who possess critical knowledge in another field such as healthcare where a combined or blended understanding of key information is integral to the industry are in short supply. In healthcare, as is the case in a host of other sectors, not only is it necessary that systems and data are protected, but the business must be compliant with existing law as well. It is imperative that action be taken to address the problem in order not to limit access to healthcare. The focus of this research is to study the serious shortage of cybersecurity professionals in the field of healthcare, the impact that this issue has on the availability of healthcare, and to suggest a solution that could provide immediate relief.

Keywords—Cybercrime, cybersecurity, fraudster, hacker, hacking, healthcare, healthcare devices, HIPAA, Health Insurance and Portability and Accountability Act, Internet of Things, IoT, medical devices, medical records, patient information, patient records

I. Overview

The focus of this work is to examine the deficit of cybersecurity professionals in healthcare, the direct and very real consequences that the shortage has on access to healthcare, and to offer a solution to the problem. [10, 22, 39] The paper contains six sections that include the *Overview*, *Introduction*, *Problem Statement*, *Proposed Solution*, *Conclusion* and *References*. The *Overview*, the Section I states the structure of the paper. Section II, the *Introduction*, provides the context for the research. Section III, *Problem Identification*, provides statistics and lays the groundwork for the discussion needed to address the shortage of cybersecurity professionals in healthcare. Section IV, *Proposed Solution*, considers a potential resolution and examines the impact on existing resources. Section V, the *Conclusion*, summarizes issues raised in the study. The sixth and final section is the *References*.

II. Introduction

The mandate for cybersecurity crosses disciplines. The deficit in the number of cybersecurity professionals required to fill current and future positions represents a growing challenge. Cybersecurity readiness presents significant ever-changing issues with possible long-term or perhaps life-threatening consequences. Cybersecurity experts who possess critical knowledge in another field such as healthcare where a combined or blended understanding of key information is integral to the industry are in short supply. In healthcare, as is the case in a host of other sectors, not only is it necessary that systems and data are protected, but the business must be compliant with existing law as well. [2, 18, 24, 43] It is imperative that action be taken to address the problem in order not to limit access to healthcare. The focus of this research is to study the serious shortage of cybersecurity professionals in the field of healthcare, the impact that this issue has on the availability of healthcare, and to suggest a solution that could provide immediate relief.

Today, a person's *digital identity* or *digital footprint* encompasses numerous multi-faceted activities and relationships. The impact extends well-beyond online purchases, credit card transactions, social media, or email, but rather spans every walk of life. An individual's *identity*, integrally related to *personally identifiable information* (PII) in the *digital space*, provides the individual with access to resources that are uniquely available to him or her. Smart-technologies combined with the *Internet of Things* (IOT) allow users to connect to online content 24/7. Comprehensive information associated with an individual such as address, place of employment, family relationships, educational history, medical records, and financial documents are available through a few screen-touches or key-strokes [21, 23].

The expansion and development of evermore robust technical infrastructure that supports continued investment in the Internet Superhighway fuels the growth in e-commerce. Mobile-computing provides avenues to virtually deliver information anywhere Internet service exists. Exponential growth in these emerging technologies provides great benefits in the way of ready access to critical services and timely conveniences. Because of enhanced infrastructure and advances in hand-held devices, in many cases, long-standing barriers to time-critical data and expertise can be eliminated. The advent of *e-medicine* is one example. Whether on the battlefield, travelling in an ambulance, moving through a medical facility or resting at home, a person's medical records are available in nearly real-time. Information that once was stored solely on paper in medical offices now

belongs to the digital realm and is transmitted across wireless networks. [2, 21, 44]

Concurrently evolving with technical advances and the benefits associated with them is the ever-increasing risk of compromise. System and data breaches are reported on a regular basis. Unfortunately, it has become common to learn of breaches at major institutions. *Ransomware*, *espionage*, *malfeasance*, *identity theft*, *phishing* represent only a few of the harmful and disruptive acts perpetrated by *fraudsters* and others who prefer to erode society. The trend shows no sign of decreasing and, in fact, is growing at an alarming rate. One consequence of the *digital-age* is the ease with which *PII* and *privacy* can be lost. Laws written and enacted to protect individuals exist. However, unforeseen results afford new and desperate challenges. [32, 43]

III. Problem Statement

The healthcare field is ripe with lucrative opportunities for *cybercriminals* to exploit. Data breaches affect the security and confidentiality of patient records [3, 4, 6, 13, 20, 28, 30, 34, 37, 44, 46, 47, 48]. HIPAA requires data protection compliance. [15] Solutions have been proposed, but the challenges are vast and diverse as is the case in other disciplines. Prevention and detection methods as well as professionally trained *cybersecurity specialists* are needed to protect patient data, medical devices and other sensitive healthcare systems. [1, 7, 8, 9, 11, 15, 19, 25, 27, 29, 31, 33, 35, 36, 38, 39, 40, 42, 45].

During a recent conversation with the Chief Security Officer (CSO) from a third-party *cybersecurity* healthcare service-provider, a critical problem in the healthcare industry came to light. The very real need exists for individuals who possess a blended education in *cybersecurity* and medical training. These *cybersecurity-medical* professionals are in extremely short supply, since every healthcare facility must have employees with this background. In addition to their responsibilities to protect and defend patient records and medical facility resources, they are required to oversee HIPAA compliance.

The discussion revealed a tragic, ethically challenging and potentially life-threatening consequence that resulted due to the shortage of *cybersecurity-medical* professionals. After acquiring a small rural hospital, a substantial regional healthcare provider was forced to close the facility for a period of time until an individual with the appropriate *cybersecurity* and medical training could be put in place. The solution for this particular problem was to hire a nurse and then send that person for training in *cybersecurity*. In the meantime, the rural community was without a local hospital while the facility remained closed.

The CSO indicated that the existing opportunities for *cybersecurity-medical specialists* are not unique to rural environments and is pervasive across the healthcare industry. In response to a request for information regarding the salary-range for individuals with *cybersecurity-medical* expertise, the answer given was $75K - $115K. Preliminary research confirms that severe shortages exist for appropriately prepared *cybersecurity-medical experts* and that the expected salary for these positions is in the stated range.

IV. Proposed Solution

Following our initial discussion with the CSO from the third-party *cybersecurity* healthcare service-provider we sought confirmation of the need for *cybersecurity-medical* professionals from additional sources that included other individuals holding similar positions and published research. [2, 14, 47]. We found not only that a shortage exists, but also that a clear appreciation for these individuals is apparent. They were referred to as *health management technology* (HMT) professionals. Included in the variety of cybersecurity issues discussed were the challenges inherent with securing the evolving and diverse landscape of medical IoT (MIoT).

The solution that we advocate is to provide a career option as an HMT professional. Individuals may opt to take this avenue from the beginning, but it also represents a great alternative for qualified students who are not accepted into a nursing program. We will examine some statistics in the paragraphs below. Currently, we are in the process of preparing a survey to learn the size of the pool of possible candidates who planned to become a nurse, but who might consider an alternate career path. Our institution offers a nursing program. We have discussed our research with colleagues in the program. We intend to conduct our survey with students enrolled in our nursing program. We have learned of another possible pool of students who intended to study physical therapy, but are not accepted into the program. We are researching its potential resource.

While the number of graduates of nursing programs has increased in recent years, particularly in BSN programs, a shortage of qualified teaching faculty, clinical sites, classroom space, budget constraints and other related issues has resulted in insufficient capacity to accommodate students in schools of nursing and many have been turned away. [5, 26, 28, 35, 41] Data in Fig. 1 and Fig. 2 reveal that the problem has continued over a period of time. Fig. 1 shows the Percentage of Programs that Turned Away Qualified Applicants by Program Type in 2012 and 2014. Fig. 2 shows the Percentage of Qualified Applicants Turned Away by Program Type in 2012 and 2014. Both sets of data are alarming, due to the fact that projections suggest the need for a greater number of nurses as baby-bombers age. [16] The data speaks for itself and indicates a troubling bottleneck in the field of nursing.

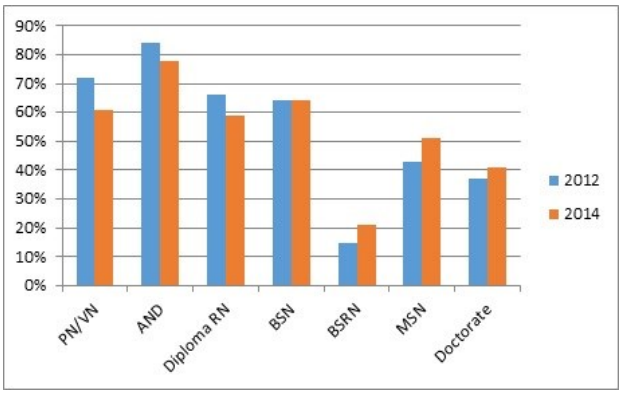

Fig. 1. Percentage of Programs that Turned Away Qualified Applicants by Program Type in 2012 and 2014 [14]

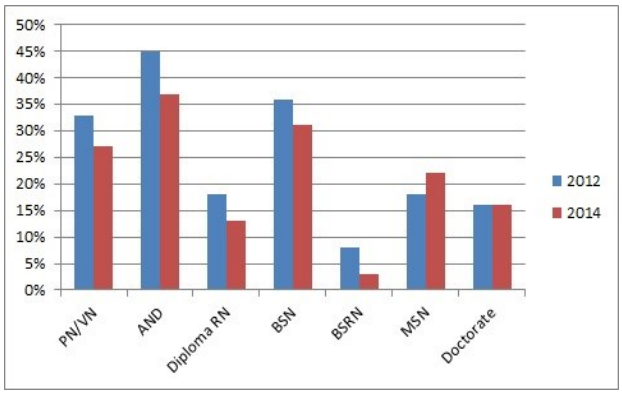

Fig. 2. Percentage of Qualified Applicants Turned Away by Program Type in 2012 and 2014 [14]

According to AACN's report on 2016-2017 Enrollment and Graduations in Baccalaureate and Graduate Programs in Nursing, U.S. nursing schools turned away 64,067 qualified applicants from baccalaureate and graduate nursing programs in 2016 due to insufficient number of faculty, clinical sites, classroom space, and clinical preceptors, as well as budget constraints. Almost two-thirds of the nursing schools responding to the survey pointed to a shortage of faculty and/or clinical preceptors as a reason for not accepting all qualified applicants into their programs. [16]

In 2017 more than 56,000 qualified nurse applicants were turned away. A sample of statistics from several institutions reveals a shortage of available educational opportunities for applicants who want to enter a nursing program. For example, from pools of 343, 262 and 200 qualified applicants, 60, 60 and 55 were accepted, respectively. Out of the pool of over 800 qualified applicants less than 200 were accepted. In other words, approximately 22% of the individuals who attempted to study nursing were able to do so, in spite of the desperate and known deficit of active nurses in the field. [26] However, the pool of applicants who were not accepted into nursing programs affords a valuable resource if one is willing to think out-of-the-box.

The solution that we advocate is to tap into the pool of qualified applicants to nursing programs who have not been accepted into programs to offer them a career option as a cybersecurity-medical professional. These students are well-prepared, possess solid GPAs of 3.5 or greater and have strong community service credentials. They are excellent candidates for a career in cybersecurity-medical opportunity. Due to the relatively few clinical slots in nursing and the significant pool of qualified students who might consider a modest career adjustment, moving these individuals in a slightly different direction in healthcare is straightforward. After completion of a number of cybersecurity classes, these students would be ready to step into a rewarding and challenging field. Further, due to the constraints outlined in publications that address issues in nursing, the pool of qualified candidates who would be suited for a career as a cybersecurity-medical I professional will remain for some time to come. [20, 25, 26]

Our suggestion affords an alternative career path to students who want to work in the healthcare field, but might not have been accepted into a nursing program. Not all potential candidates will decide to shift to cybersecurity, but some will. This is good for the student and benefits medical facilities that depend on cybersecurity-medical specialists to protect patient data, computer systems and medical devices as well as ensure that compliance with Federal Law is maintained. Finally, our suggestion does not affect the field of nursing in an adverse way, because it does not diminish the pool of nursing student applicants. Rather it utilizes valuable resources that remain in the pool. It is a win for everyone involved.

V. Conclusion

Opportunities as *cybersecurity-medical* professionals are widespread in the healthcare industry. Responsibilities include the protection of critical patient information and key infrastructure. The deficit in the number of adequately prepared individuals who are ready to meet these challenges represents a significant vulnerability to the healthcare system on multiple fronts. We offered a potential solution to help to mitigate the problem. Given the strong interest in the healthcare field as a career path due to the solid earning potential and the continued high demand for qualified *cybersecurity* professionals, blended *cybersecurity-medical specialist* opportunities represent an option for well-prepared and motivated individuals. Certainly not every qualified applicant to a nursing or physical therapy program that is not accepted will elect to move in a different direction to pursue a career in *cybersecurity*, but some will. It is our hope that programs can be developed to prepare students for challenging and rewarding careers as *cybersecurity-medical* professionals. The need is great as is the opportunity to make a difference. A focus to address the critical shortage of *cybersecurity-medical specialists* will be of benefit to all parties, the individual, medical facility and community. It is a win all the way around.

References

[1] Adams-Collman J., Ransomware and cyber security: the king that did not wannacry, Prim Dent J. 2018 Mar 1;7(1):44-47. doi: 10.1308/205016818822610307.

[2] Atkins, S., Lawson, C., "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure". Public Administration Review. 2021;81(5):847-861. doi:10.1111/puar.13322

[3] Bachiri M, Idri A, Fernández-Alemán JL, Toval A., "Evaluating the privacy policies of mobile personal health records for pregnancy monitoring", J Med Syst. 2018 Jun 29;42(8):144. doi: 10.1007/s10916-018-1002-x.

[4] Baranchuk A, Alexander B, Campbell D, Haseeb S, Redfearn D, Simpson C, Glover B., "Pacemaker cybersecurity", Circulation. 2018 Sep 18;138(12):1272-1273. doi: 10.1161/CIRCULATIONAHA.118.035261.

[5] Buerhaus, P., Auerbach, D.,Staiger, D., "Recent changes in the number of nurses graduating from undergraduate and graduate programs", Nursing Economics,January-February 2016; 34(1): 46-48.

[6] Bhimji SS, Hackert PB., "Patient confidentiality", StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2018 Jan 2018 Aug 9.

[7] Brogan J, Baskaran I, Ramachandran N., "Authenticating health activity data using distributed ledger technologies", Comput Struct Biotechnol J. 2018 Jul 17;16:257-266. doi: 10.1016/j.csbj.2018.06.004. eCollection 2018.

[8] Burhan M, Rehman RA, Khan B, Kim BS., "IoT elements, layered architectures and security issues: a comprehensive survey", Sensors (Basel). 2018 Aug 24;18(9). pii: E2796. doi: 10.3390/s18092796.

[9] Chen J, Ge H, Moore S, Yang W, Li N, Proctor RW., "Display of major risk categories in android apps", J Exp Psychol Appl. 2018 Sep;24(3):306-330. doi: 10.1037/xap0000163. Epub 2018 Jun 21.

[10] Chua, JA., "Cybersecurity in the Healthcare Industry – A Collaborative Approach"., Physician Leadership Journal. 2021;8(1):23-25.

[11] Chuang YH, Lo NW, Yang CY, Tang SW., "A lightweight continuous authentication protocol for the internet of things", Sensors (Basel). 2018 Apr 5;18(4). pii: E1104. doi: 10.3390/s18041104.

[12] Cohen IG, Mello MM., "HIPAA and protecting health information in the 21st Century", JAMA. 2018 Jul 17;320(3):231-232. doi: 10.1001/jama.2018.5630.

[13] Coventry L, Branley D., "Cybersecurity in healthcare: a narrative review of trends, threats and ways forward", Maturitas. 2018 Jul;113:48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22.

[14] "Cyberattack Disruptions May Put Patient Safety at Risk" HTM & Capital Equipment Purchasing: How healthcare management professionals are playing a key roles in procuring the equipment hospitals need". 24 X 7. 2018; 23(7):18-21

[15] Edemekong PF, Haydel MJ., "Health insurance portability and accountability act (HIPAA)", StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2018 Jan-.2018 May 13.

[16] "Fact sheet: nursing shortage," American Association of Colleges of Nursing, https://www.aacnnursing.org/Portals/42/News/Factsheets/Nursing-Shortage-Factsheet.pdf, September 2020

[17] "Findings from the 2014 NLN biennial survey of schools of nursing academic year 2013-2014: executive summary. (headlines from the NLN) (national league of nursing)", Nursing Education Perspectives, 2015, vol. 36(6),p. 425(2)

[18] Ganin, A., Quach, P., Panwar, M., et al., "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management"., Risk Analysis: An International Journal., 2020;40(1):183-199. doi:10.1111/risa.12891

[19] Goedert J., "Boosting security for devices organizations try to close 'back doors' to their networks", Health Data Management 2017, May;25(2):42-43, https://pubmed.ncbi.nlm.nih.gov/29799679/

[20] Gostin LO, Halabi SF, Wilson K., "Health data and privacy in the digital era.", JAMA. 2018 Jul 17;320(3):233-234. doi: 10.1001/jama.2018.8374. Health Data Manag. 2017 May;25(2):42-43.

[21] Hamilton-Basich, M., "Are You Sure Your Devices Are Secure?"., 24 X 7., 2021 Aug/Sept, Vol 26, I(6);10-12,

[22] Hayhurst, C., "HTM & Capital Equipment PURCHASING: How healthcare professionals are playing key roles in procuring the equipment hospitals need"., 24 7. 2018;23(7):18-21.

[23] Howard, D., Harris, CR., "Cybersecurity: What Leaders Must Know". Physician Leadership Journal. 2019;6(4):49-53.

[24] Hutchison, V., Brackett, J., "Cybersecurity and fire protection: Is your system a pathway for internet attacks?"., Health Facilities Management., 2021;34(4):26-29.

[25] Jalali MS, Kaiser JP., "Cybersecurity in hospitals: a systematic, organizational perspective", J Med Internet Res. 2018 May 28;20(5):e10059. doi: 10.2196/10059.

[26] Kavilanz, P., "Nursing schools are rejecting thousands of applicants – in middle of a nursing shortage" , https://money.cnn.com/2018/04/30/news/economy/nursing-school-rejections/index.html

[27] Ko H, Měsíček L, Choi J, Hwang S, "A study on secure medical-contents strategies with drm based on cloud computing", *J Healthc* Eng. 2018 Mar 29;2018:6410180. doi: 10.1155/2018/6410180. eCollection 2018.

[28] Kobayashi S, Kane TB, Paton C., "The privacy and security implications of open data in healthcare",Yearb Med Inform. 2018 Aug;27(1):41-47. doi: 10.1055/s-0038-1641201. Epub 2018 Apr 22.

[29] Kumar V, Jangirala S, Ahmad M., "An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing", J Med Syst. 2018 Jun 28;42(8):142. doi: 10.1007/s10916-018-0987-5.

[30] Langarizadeh M, Orooji A, Sheikhtaheri A., "Effectiveness of anonymization methods in preserving patients' privacy: a systematic literature review", Stud Health Technol Inform. 2018;248:80-87.

[31] Levitin G, Xing L, Huang HZ., "Security of separated data in cloud systems with competing attack detection and data theft processes", Risk Anal. 2018 Oct 12. doi: 10.1111/risa.13219. [Epub ahead of print]

[32] Liu, C-W., Huang, P., Lucas, HC., "Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions". Journal of Management Information Systems. 2020;37(3):758-787.doi:10.1080/07421222.2020.

[33] Maisel WH, Paulsen JE, Hazelett MB, Selzman KA., "Striking the right balance when addressing cybersecurity vulnerabilities", Heart Rhythm. 2018 Jul;15(7):e69-e70. doi: 10.1016/j.hrthm.2018.05.002. Epub 2018 May 10.

[34] Mertz L., "Cyberattacks on devices threaten data and patients: cybersecurity risks come with the territory. three experts explain what you need to know" , IEEE Pulse. 2018 May-Jun;9(3):25-28. doi: 10.1109/MPUL.2018.2814258.

[35] Mozzaquatro BA, Agostinho C, Goncalves D, Martins J, Jardim-Goncalves R., "An ontology-based cybersecurity framework for the internet of things" , Sensors (Basel). 2018 Sep 12;18(9). pii: E3053. doi: 10.3390/s18093053.

[36] Murphy SP., "A holistic approach to cybersecurity starts at the top", Front Health Serv Manage. 2018 Fall; 35(1):30-36. doi: 10.1097/HAP.0000000000000041.

[37] Paulsen JE, Hazelett MB, Schwartz SB., "Cied cybersecurity risks in an increasingly connected world", Circulation. 2018 Sep 18;138(12):1181-1183. doi: 10.1161/CIRCULATIONAHA.118.035021.

[38] Peterson DC, Adams A, Sanders S, Sanford B., "Assessing and addressing threats and risks to cybersecurity", Front Health Serv Manage. 2018 Fall; 35(1):23-29. doi: 10.1097/HAP.0000000000000040.

[39] Pycroft L, Aziz TZ., "Security of implantable medical devices with wireless connections: the dangers of cyber-attacks", Expert Rev Med

Devices. 2018 Jun; 15(6):403-406. doi: 10.1080/17434440.2018.1483235. Epub 2018 Jun 13.

[40] Reagin MJ, Gentry MV., "Enterprise cybersecurity: building a successful defense program", Front Health Serv Manage. 2018 Fall; 35(1):13-22. doi: 10.1097/HAP.0000000000000037.

[41] Salsberg, E., "Recent Trends in the Nursing Pipeline: US Educated BSNs Continue to Increase", https://www.healthaffairs.org/do/10.1377/hblog20150409.046241/full/

[42] Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE., "Factors influencing the decision to proceed to firmware upgrades to implanted pacemakers for cybersecurity risk mitigation"., Circulation. 2018 Sep 18;138(12):1274-1276. doi: 10.1161/CIRCULATIONAHA.118.034781.

[43] Scala, NM., Reilly, AC, Goethals, PL., Cukier, M., "Risk and the Five Hard Problems of Cybersecurity". Risk Analysis: An International Journal. 2019;39(10):2019-2126.doi:10.1111/risa.13309.

[44] Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M., "The evolving state of medical device cybersecurity", Biomed Instrum Technol. 2018 Mar/Apr;52(2):103-111. doi: 10.2345/0899-8205-52.2.103.

[45] Sheffer J., "Frontlines: every piece counts in cybersecurity", Biomed Instrum Technol. 2018 Mar/Apr;52(2):82-83. doi: 10.2345/0899-8205-52.2.82.

[46] Slotwiner DJ, Deering TF, Fu K, Russo AM, Walsh MN, Van Hare GF., "Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians", Proceedings of the Heart Rhythm Society's Leadership Summit.

[47] Smith C., "Cybersecurity implications in an interconnected healthcare system", Front Health Serv Manage. 2018 Fall;35(1):37-40. doi: 10.1097/HAP.0000000000000039.

[48] Zelmer J., "Cybersecurity in Health: A 21st-Century Imperative", Healthcare Policy., 2018 May;13(4):6-10. doi: 10.12927/hcpol.2018