Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis

By Liu Hua Yeo, MS, and James Banfield, PhD

Abstract

The healthcare sector continues to be the industry suffering one of the highest costs of a data security breach. Healthcare lags behind other industries in cybersecurity preparedness despite advances in cybersecurity technologies. Technical safeguards to protect electronic health records must be combined with human behavioral interventions to promote a robust cybersecurity plan. Using data from the United States Department of Health and Human Services, we conducted an exploratory analysis of past data breaches in healthcare organizations from January 2015 to December 2020 to explore the extent to which human elements played a role in data security incidents. We found that a vast majority of health records were compromised due to poor human security. The mean number of records affected by a breach due to unintentional insider threats is more than twice that of breaches caused by malicious intent such as external cyberattacks and theft. Our findings also indicate that, on average, more patient records are compromised from falling for a phishing scam than any other reason. We argue that proper cybersecurity contingency plans in healthcare must include human behavioral interventions that go beyond technical controls.

Keywords: cybersecurity, healthcare breaches, human factors, insider threats

Introduction

The digitization of medical records has changed the landscape of healthcare systems worldwide. With the advent of the information age, paper-based healthcare records were gradually and systematically converted into digitized electronic health records (EHRs). In the last two decades, the push toward resource sharing in technology is revolutionizing the healthcare sector by providing an efficient way of sharing patient records between healthcare professionals. Compared to paper-based records, EHRs require less manpower, time, and physical storage. Caregivers and providers use EHRs to access care-related activities and provide evidence-based decision support and quality care.[1] However, the ease of access to EHRs is accompanied by rising cybersecurity threats and challenges.

In the annual "Cost of Data Breach" report conducted by the Ponemon Institute, the 2020 study noted that each compromised record cost an average of $146 to the healthcare organization (HCO). That figure increases to $150 per compromised record where personal health information (PHI) was involved. According to the report, healthcare continues to be the industry suffering the highest cost of a data breach at $7.13 million when factoring in other costs such as incident response, lost business, and notification costs. Eighty percent of the breached organizations participating in the study reported that PHI was involved. The cost of healthcare breaches is expected to increase during the COVID-19 pandemic, as 76 percent of HCOs in the survey predicted that implementing an incident response strategy will be made much more difficult by the ubiquity of remote work during the pandemic.[2] Most healthcare executives lack overall information security, employee security awareness, and incident response strategies.[3] Breaches related to EHR can significantly affect HCOs, such as the accidental release of PHI to

disruptions in clinical care.[4-6] Disruptions and delays in patient care can result in patient death, and the impact on patient safety is likely to be underreported.[7]

Federal compliance laws such as Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act were enacted to require the adoption of electronic medical records and protect privacy and data security of PHI.[8]As required by section 13402 (e) (4) of the HITECH Act, The United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The HIPAA Security Rule requires healthcare organizations and covered entities protect electronic personal health information from cybersecurity threats.[9] It also imposes administrative, technical, and physical standards for safeguards that organizations must implement. These entities must implement data security safeguards to protect PHI, such as medical records and insurance information. This paper presents an exploratory analysis of past EHR breaches in the United States from 2015to 2020. By exploring the factors that led to violations, executives and decision-makers in HCOs can apply lessons from these breaches in securing their organizations.

Research Question

We investigated the extent to which the lack of proper human security enabled data breaches in HCOs. Our research questions were thus:

1. To what extent did the lack of human security result in data security breaches in healthcare records?
2. On average, how does the lack of human security affect the number of records breached in a cybersecurity incident in healthcare?

We hypothesized that data breaches in healthcare caused by unintentional human factors, such as carelessness, negligence, and falling victim to phishing and ransomware, outnumber those caused by malicious intent. The following sections discuss our observational study results and help research determine solutions for incorporating human security into organizational policies. We argue that any security framework must emphasize securing the human in HCOs.

Classification Method

We conducted an exploratory study on the factors that play a role in EHR-related cybersecurity breaches. HCOs are required by law to notify the OCR after a breach compromising EHRs and PHIs. The OCR publishes details of these reported breaches beginning October 2009 and makes the dataset publicly available.[10] It includes reports from HCOs that have suffered breaches that compromised 500 or more EHRs. Since the law requires HCOs to notify HHS in the event of a violation, we believe that this nationwide sample is sufficiently representative of the population of EHR-related breaches in healthcare, with some limitations. Our analysis used a methodology based on the Joanna Briggs Institute (JBI) approach, which provides an evidence-based process for qualitative research.[11] We modified a similar method by Walker-Roberts et al.[12] in our classification process. **Figure 1** shows a graphical representation of the flow process, which describes how we identified and screened each entry in our dataset for inclusion in the exploratory analysis. Our criteria for inclusions were that entries:

- Included valid and clear descriptions of the breach incident.
- Occurred between January 1, 2015, and December 31, 2020, inclusive
- Constituted a breach as defined under HIPAA. Entries alleging violations by entities not covered under HIPAA, or those determined by OCR to have not violated any HIPAA rules, were excluded.

We limited our analysis of the OCR dataset to the years spanning January 2015 to December 2020; after removing incomplete records and other entries that do not constitute a breach of PHI, the resulting set of data contained 1,485 security incidents. The data was then analyzed to determine the type of the cybersecurity breach. Entries were categorized based on the presence or absence of malicious intent. In 15 cases, we could not establish those criteria based on the incident descriptions provided in the original dataset. These cases were noted with an "Insufficient information" designation. Once the type of breach has been identified, we further classified each entry into the primary source or cause of the breach for analysis. **Table 1** describes in detail our classification methods for each entry.

Results and Discussion

We studied 1,485 breach events occurring between January 2015 and December 2020, affecting 141,252,797 medical records. Of that number, 73.1 percent of all affected records resulted from breaches caused by unintentional factors, while 26.7 percent were caused by malicious factors. **Figure 2** shows the resulting classification of thesources of EHR breaches in HCOs and their frequency of occurrence in the United States from January 2015 to December 2020. We found the most frequent reason for a cyber breach in HCOs is the result of carelessness and negligence (382 incidents), followed by theft (222 incidents), and falling victim to a phishing scam (221 incidents). Similarly, **Table 2** shows the total number of records affected by each breach categories based off our classification method.

Carelessness/Negligence

Existing literature on insider threats generally assumes that individuals who commit cybersecurity transgressions do so due to an ulterior motive that is typically accompanied by malicious intent or the desire to enrich themselves for financial or personal gain.[13] However, our dataset analysis revealed that 382 incidents, or 26 percent of all human factor-based breaches, were due to an insider's carelessness, negligence, or apathy. In each of these cases, no malicious intent was visible in that there was no intent to access patient data, but a data breach occurred. Employees or business associates may partake in risky cybersecurity behaviors due to a highrisk tolerance or the desire to be efficient or helpful.[14] In some cases, employees may inadvertently circumvent established policies because they view those policies as cumbersome or unrelated to patient outcomes.[15] This paper does not intend to define a framework for what constitutes an insider threat but rather to show that carelessness and negligence stemming from risky behaviors, lack of awareness, and apathy are essential domains of human security.

Of the 382 incidents stemming from carelessness or negligence, 212 (55.5 percent) were incidents whereby an employee or business associate erroneously mailed or emailed PHI to the wrong recipients. Some were caused by misalignment in the printing process or information

mismatched with patient data. In other cases, PHI may have been mailed to the correct recipients but done so in a manner that unintentionally exposed the PHI in transit.

Misplaced hard drives or documents containing PHI lost in the mail or transit were described in 71 incidents. In most of these cases, the covered entities never recovered the lost records. According to the dataset, some of these losses were attributed to carelessness on behalf of an employee. We note that we did not include cases where external individuals deliberately stole PHI during a burglary; these entries were classified under the "Theft" source of breach category due to the clear presence of malicious intent. These cases are therefore distinguished from incidents where PHI was lost due to negligence or carelessness. In a further 59 incidents, PHI was unintentionally and improperly exposed by individuals who uploaded the data onto publicly accessible websites or databases without taking security steps such as encrypting or sanitizing the data beforehand.

These accidental transgressions led to tangible consequences for both the offending employee(s) and the organization. According to the HHS dataset, consequences included penalties ranging from reprimand and retraining of the individual(s) to the suspension or termination of employment, depending on the severity and impact of the risky behavior. In addition, under HIPAA, organizations face substantial fines for noncompliance with the HIPAA Privacy Rule. In a February 2022 update, the OCR noted that since the compliance date of the Privacy Rule in April 2003, it has imposed civil penalties totaling $131 million to organizations for non-compliance.[16]

Phishing/Ransomware

Falling victim to a phishing scam made up most of the number of EHRs affected in our dataset. There were 221 incidents directly attributed to phishing scams, and 119 reported breaches were related to ransomware. Together, they make up 40.7 percent of all non-malicious events in our chosen time range. Our analysis combined phishing and ransomware incidents because a cybersecurity victim's vector to produce that outcome is similar. Phishing, which is the act of tricking a user into disclosing confidential information[17] through a legitimate-looking email or link, is the vehicle that delivers the ransomware payload.[18]

In a phishing attack, one compromised credential can lead to multiple subsequent attacks, as we saw in Anthem Inc. in 2015,[19] whereby a targeted spear-phishing campaign opened the door to further parts of its network. During the attack, 78,800,000 affected records were attributed to Anthem's breach incident as corroborated by the OCR dataset. Anthem had disclosed that it had suffered a data breach that affected almost 80 million customers.[20,21] Anthem discovered that the attackers had managed to obtain several employees' credentials, possibly through a phishing attack in their investigation. Once the attackers had obtained the credentials, they ran several data queries between December 2014 and January 2015. The database credentials would then be trivial to access using the stolen credentials.[22] Eventually, the attackers could access Anthem's enterprise data warehouse containing personally identifiable information (PII) and stole almost 80 million unique user records.[23]

Although the Anthem incident may seem like a statistical outlier, we argue that, on the contrary, it further underscores the gravity of falling victim to a phishing attack. One phishing incident led to the most significant cybersecurity breach in the healthcare industry. Victims of phishing, ransomware, and other social engineering attacks become a new vector or vehicle to launch more

in-depth and large-scale attacks.[24] Once in the system, the attackers ran queries and worked from there to gain higher-level access. The Anthem administrator who found the breach noticed that his password was used to run queries that he did not initiate.[25] The ability for an administrator's password to be used in this manner points to a possible flaw in Anthem's data management policy; actions executed by elevated privilege accounts should always be accompanied by some form of additional verification or authentication beyond a simple password requirement. While it cannot be said definitively that the presence of an additional authentication factor would have prevented the breach, it would have been an extra layer of defense against the attack.

Malicious Insider

Malicious insiders refer to individuals with knowledge or access to internal systems or networks, who then commit cybersecurity crimes with the express intent of enriching themselves for financial, personal, or other gains.[26,27] As we noted earlier in this paper, the allure of economic gains from PHI on the black market may drive individuals to commit cybercrime. However, malicious insiders may have motives other than profit, such as disgruntled employees attempting to exact revenge for a perceived wrong or a sense of entitlement. Cybersecurity controls typically are designed to thwart external attacks, and there are few, if any, technical controls that specifically defend against internal threats.[28] Insiders have a crucial advantage: They are generally knowledgeable about systems and processes in the organization and may have varying administrative access levels that external actors do not.

To illustrate this, we found that in our analysis of the OCR dataset, there were 217 incidents of malicious insiders, affecting a total of 55,199,447 records. In as many as 170 of these cases, employee(s) of the HCO accessed PHI without a legitimate business need.

Other Sources of Breach

Under the "Unintentional" type category, the source of a breach in a total of 32 incidents was something other than the abovementioned categories. Since there were relatively few of these, we combined and classified these entries as "Other" in our analysis. In three incidents, the breaches were caused by employees falling for a social engineering attack. Social engineering, which is an umbrella term that includes phishing and ransomware, describes a process whereby an attacker uses social interaction to deceive and obtain sensitive information from a victim.[29-31] For instance, an attacker may pose as an authorized individual and trick a user into divulging credentials to an internal network. In the OCR dataset, due to the prevalence of healthcare breach incidents caused by falling victim to phishing or ransomware attacks, we distinguished these categories from the more broadly applicable social engineering category. Ten incidents in the "Other" category stemmed from a lack of a business associate agreement between a covered entity and its business associate. Under the HIPAA Rules, a business associate agreement must be executed to ensure that any business entity that establishes a relationship with a covered HCO will commit to safeguarding PHI. Other incidents include breaches due to miscellaneous policy violations (eight occurrences), unintentional physical exposure of PHI (five occurrences), easily guessed passwords (four), and natural disasters (two).

Across all incidents, the OCR dataset shows that from 2015 to 2020, the mean number of records affected by unintentional factors is 123,446, more than twice that of the mean caused by malicious factors. **Figure 3** shows the mean number of records affected when considering the type of breach. A closer look at the subfactors shows that phishing and cyberattacks led to the

highest mean number of records affected at 421,038 and 153,644 records. **Figure 4** breaks those categories down further into its subcategories based off our classification method and shows the mean number of records affected by each subcategory.

Conclusion

As healthcare services evolve in technology and coverage, they aim to provide a variety of treatments in order to accommodate diverse patient demographics. This was especially noticeable with the influx of patients impacted by the COVID-19 global pandemic. Due to the volatile and unpredictable nature of the virus, healthcare providers were forced to find alternative means of treatment in order to adequately provide necessary services to their patients. This included an increase of services, which entailed the usage of tools such as technology through cloud-based data inference, surveys, COVID-19 screening symptom checklists, and virtual appointment services. Such alternative means of seeking treatment were designed to minimize risk of exposure to patients, healthcare providers, and workers. With the increase in telehealth services, many healthcare workers began to perform remote work during the pandemic.[32] The Federal Bureau of Investigation (FBI) have reported that cyberattacks have increased almost 400 percent by the first few months of the pandemic.[33] In addition, the rise of telehealth means that many remote employees are now using their personal computers and home networks to perform their jobs. HCOs with essential workers working on-site are also grappling with the necessity of "bring your own device" (BYOD) policies to maintain patient care and outcome pre-pandemic. Working remotely means that HCOs have to deal with significant amounts of data being sent over the network off-premises in remote locations. In addition to expanding the attack surface for cyber criminals to take advantage of,[34,35] these developments and decentralized resources also increase the risk of accidental exposure of PHI as telehealth signals a necessary paradigm shift in providing patient care.

Data breaches in healthcare are incredibly lucrative as pathways to identity theft on the black market. According to Verizon's latest data breach report, published in May 2021, 85 percent of all breaches involved a human element, and during the COVID-19 global pandemic, phishing continued to be one of the most commonly employed methods in a data security incident across all industries. The report also indicated that ransomware has jumped to third place in terms of the most frequently occurring source of breaches. Similarly, the Healthcare Information and Management Systems Society (HIMSS) released a survey report stating that phishing is the most common attack vector in healthcare.[36] This finding is consistent with our discovery with the OCR dataset. We showed that, on average, more EHRs are compromised to a phishing scam (mean of 421,938 records affected) than any other reason. We also noted that in the time range of our analysis, carelessness, negligence, and phishing were the most frequently occurring sources of EHR breaches.

The discourse on data breaches and EHR exposure has changed from "if" to "when" an HCO will experience a data breach. Based on our observational study of the OCR dataset, threats involving human elements continue to be significant risk factors for EHR breaches. An organization's ability to train and impart information awareness to its employees' behaviors is paramount in the fight against cybersecurity attacks on HCOs. A survey conducted in Germany by PricewaterhouseCoopers (PwC) revealed that a staggering 87 percent of participants believe that better education for medical staff is crucial to an HCO's cybersecurity hygiene.[37] Phishing

as a security incident is not new, yet the fact that it remains one of the most common occurrences of data breaches suggests that it may not be taken as seriously as it should be. Organizational data security policies may not receive widespread compliance in an HCO because employees may not perceive the risk of poor cybersecurity hygiene. An effective information awareness and training program must do more than simply transfer knowledge about proper behavior in cybersecurity. Incorporating behavioral science into training programs to change deeply rooted online habits is crucial in combating human-influenced breaches such as carelessness and phishing.[38-40] Technical safeguards should not be the only avenue to accomplish this goal; rather, it needs to be bolstered by the cyber vigilance of human elements.[41] There is no one holy grail of countermeasures sufficient to prevent human risks that lead to cyberattacks. Each HCO must conduct its own risk assessment that accounts for resource constraints and the feasibility of such methods.[42]

Our analysis of the data breaches in healthcare as reported to HHS has identified several contributing factors. As we have observed, many of the cases we analyzed involved unintentional insider threats, and these cases lead to significant loss and exposure of EHR. This analysis was informative in specifying directions for future research and areas to focus on in mitigating cyber-attacks.

Notes

1. Kruse CS, Frederick B, Jacobson T, Monticone DK. "Cybersecurity in healthcare: A systematic review of modern threats and trends." *Technology & Health Care*. 2017;25(1):1-10. doi:10.3233/THC-161263

2. "Cost of a Data Breach Report 2020." Ponemon Institute LLC; 2020. https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

3. Castelli C, Gabriel B, Yates J, Booth P. "Strengthening digital society against cyber shocks: Key findings from The Global State of Information Security® Survey 2018." *Cybersecurity and Privacy*. Published online 2017:22.

4. Gordon WJ, Fairhall A, Landman A. "Threats to Information Security - Public Health Implications." *N Engl J Med*. 2017;377(8):707-709. doi:10.1056/NEJMp1707212

5. Jalali MS, Russell B, Razak S, Gordon WJ. "EARS to cyber incidents in health care." *J Am Med Inform Assoc*. 2019;26(1):81-90. doi:10.1093/jamia/ocy148

6. Bhuyan SS, Kabir UY, Escareno JM, et al. "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations." *Journal of Medical Systems*. 2020;44(5). doi:10.1007/s10916-019-1507-y

7. "2020 HIMSS Cybersecurity Survey." Healthcare Information and Management Systems Society; 2020. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf

8. Koch DD. “Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?” *Journal of Health Care Finance*. 2016;43(3). Accessed March 10, 2021. https://healthfinancejournal.com/index.php/johcf/article/view/67

9. Kosseff J. “Cybersecurity Requirements for Specific Industries.” In: *Cybersecurity Law*. 2nd ed. John Wiley & Sons, Ltd; 2020.

10. “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.” U.S. Department of Health & Human Services - Office for Civil Rights. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=48C4A2DEB0F6F4053924B40BF2B12B12

11. Aromataris E, Munn Z, eds. *JBI Manual for Evidence Synthesis*. JBI; 2020. doi:10.46658/JBIMES-20-01

12. Walker-Roberts S, Hammoudeh M, Dehghantanha A. “A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure.” *IEEE Access*. 2018;6:25167-25177. doi:10.1109/ACCESS.2018.2817560

13. Hadlington L. “The “Human Factor” In Cybersecurity: Exploring the Accidental Insider.” In: *Psychological and Behavioral Examinations in Cyber Security*. 1st ed. IGI Global; 2018:46-63.

14. CERT. “Unintentional Insider Threats: A Foundational Study.” Software Engineering Institute; 2013.

15. Mansfield-Devine S. “Leaks and ransoms – the key threats to healthcare organisations.” *Network Security*. 2017;2017(6):14-19. doi:10.1016/S1353-4858(17)30062-4

16. Office for Civil Rights. Enforcement Highlights. HHS.gov. Published February 28, 2022. Accessed March 16, 2022. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

17. Barrett MP. “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.” *NIST Cybersecurity Framework*. Published online April 16, 2018. doi:10.6028/NIST.CSWP.04162018

18. Croke L. “Protecting your organization from e-mail phishing and ransomware attacks.” *AORN Journal: The Official Voice of Perioperative Nursing*. 2020;112(4):P10-P12. doi:10.1002/aorn.13229

19. “Anthem breach traced to admin’s stolen login.” *Healthcare Risk Management; Atlanta*. 2015;37(3). Accessed February 22, 2021. http://search.proquest.com/docview/1987263449/abstract/37CE188769A0479DPQ/1

20. Mathews AW. “Anthem: Hacked Database Included 78.8 Million People.” *Wall Street Journal*. https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364. Published February 24, 2015. Accessed April 19, 2021.

21. Riley C. “Insurance giant Anthem hit by massive data breach.” CNNMoney. Published February 4, 2015. Accessed March 22, 2021. https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html

22. “Anthem breach traced to admin’s stolen login.” *Healthcare Risk Management; Atlanta*. 2015;37(3). Accessed February 22, 2021. http://search.proquest.com/docview/1987263449/abstract/37CE188769A0479DPQ/1

23. Miller NA. “Report of the Multistate Targeted Market Conduct and Financial Examination.” Alvarez & Marsal Insurance and Risk Advisory Services, LLC; 2016.

24. Gyunka BA, Christiana AO. “Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary.” *Computing & Information Systems*. 2017;21(2):10-18.

25. McGee MK. “A New In-Depth Analysis of Anthem Breach.” Published January 2017. Accessed May 5, 2021. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

26. Greitzer FL. “Insider Threats: It’s the HUMAN, Stupid!” In: *Proceedings of the Northwest Cybersecurity Symposium*. ACM; 2019:1-8. doi:10.1145/3332448.3332458

27. Homoliak I, Toffalini F, Guarnizo J, Elovici Y, Ochoa M. “Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures.” *ACM Comput Surv*. 2019;52(2):30:1-30:40. doi:10.1145/3303771

28. Greitzer FL. 2019.

29. Aldawood H, Skinner G. “Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues.” *Future Internet*. 2019;11(3):73. doi:10.3390/fi11030073

30. Guitton MJ. “Cybersecurity, social engineering, artificial intelligence, technological addictions: Societal challenges for the coming decade.” *Computers in Human Behavior*. 2020;107:106307. doi:10.1016/j.chb.2020.106307

31. Salahdine F, Kaabouch N. “Social Engineering Attacks: A Survey.” *Future Internet*. 2019;11(4):89. doi:10.3390/fi11040089

32. Kim L. “Cybersecurity and related challenges during the COVID-19 pandemic.” *Nursing*. 2021;51(2):17-20. doi:10.1097/01.NURSE.0000731916.83045.e6

33. Miller M. “FBI sees spike in cyber crime reports during coronavirus pandemic.” TheHill. Published April 16, 2020. Accessed November 13, 2021. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

34. Kim L. “Cybersecurity and related challenges during the COVID-19 pandemic.” *Nursing*. 2021;51(2):17-20. doi:10.1097/01.NURSE.0000731916.83045.e6

35. Internet Crime Complaint Center. *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*. Federal Bureau of Investigation; 2020. doi:10.6028/NIST.SP.800-46r2

36. *2021 HIMSS Cybersecurity Survey*. Healthcare Information and Management Systems Society; 2022. Accessed March 30, 2022. https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf

37. von Grätz PG. "The real cybersecurity risk sits between the chair and keyboard." Healthcare IT News. Published October 3, 2019. Accessed April 4, 2021. https://www.healthcareitnews.com/news/europe/risk-between-chair-and-keyboard

38. CERT. *Unintentional Insider Threats: A Foundational Study*. Software Engineering Institute; 2013.

39. Bada M, Sasse AM, Nurse JRC. "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?" *arXiv:190102672 [cs]*. Published online January 9, 2019. Accessed April 28, 2021. http://arxiv.org/abs/1901.02672

40. *Verizon 2021 Data Breach Investigations Report*. Verizon; 2021. https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

41.Greitzer FL. 2019.

42.CERT. *Unintentional Insider Threats: A Foundational Study*. Software Engineering Institute; 2013.

Author Biographies

Liu Hua Yeo (lyeo@emich.edu) is a PhD candidate in cybersecurity at Eastern Michigan University. His research interests include risk factors in healthcare cybersecurity.

James Banfield (jbanfield@emich.edu) is an associate professor of cybersecurity at the School of Information Security and Applied Computing at Eastern Michigan University.