Designing an Effective Organizational Culture to Guard Against the Cyber Risks of Emerging Technologies

Megan E. Watkins

Auburn University
Health Services Administration Program

Executive Summary

The Internet of Medical Things (IoMT) and interoperable technologies have transformed how patient data impacts medical care; such technological innovation revolutionizes how HCOs improve cost, quality, and access. New cyber risks, however, accompany developing cyber ecosystems. Although immediate data exchange is beneficial, risk arises from IoMt's increased susceptibility to human influence. The success of quality care relies on protecting the operationality of Health Information Technology (HIT) against newly developing cyber vulnerabilities. Therefore, management must be just as invested in their HCO's cybersecurity protocols as cybercriminals are in bypassing those protocols. This essay proposes a Healthcare Cyber Resiliency Model (HCRM) that leverages human and technical factors through an iterative cycle of feedback and process improvement. It intends to equip healthcare administrators with a foundational philosophy necessary to progress further in securing their emerging technologies.

Designing an Effective Organizational Culture to Guard Against the Cyber Risks of Emerging Technologies

The pressures of the COVID-19 pandemic have accelerated a transition to complete digitization, in which cloud servers and hybrid network structures offer seamless data-sharing capabilities that resolve the divide between outdated information systems and the transformation of the traditional consumer to a digitally literate end-user (Tarikere et al., 2021). The healthcare sector increasingly relies on interoperable information technology (IT) applications to securely manage, store, and share private patient information that the appropriate clinicians can promptly access. Consequently, network vulnerabilities have positioned healthcare organizations (HCOs) to become victims of crippling, recurring, and costly cyberattacks, with a documented 125% increase since 2015 (Abraham et al., 2019). Alarmingly, this reveals that HCOs' conventional cybersecurity strategies are painfully inadequate against rapidly evolving cyberattacks that directly exploit newly adopted interoperable technologies to endanger patient privacy and safety.

As a health administrator, it is imperative to gain further insight into the impact of cyberattacks on HCOs. Such insight includes understanding modern cyberbreach strategies and traditional detection methods in response to attacks and contextualizing the development of interoperable systems to explain their enhanced cyber risks. In addition, discussing the significant impact of human factors on cyberattacks and implementing a multifaceted organizational strategy that leverages technology and human factors is critical. As a result, this essay will examine the significance of a comprehensive approach to protecting the operationality of health information Technology (HIT) systems against evolving cybercrimes targeting newly developing vulnerabilities that negatively impact patient care.

Overview of Cyberattacks and Breaches

Cyberattacks are “any kind of malicious activity that attempt to collect, disrupt, deny, degrade, or destroy information system resources or the information itself” (*Cyberattack - glossary: CSRC).* A cyberbreach is a specific cyberattack “…when information is lost, stolen, displaced, hacked, or communicated to unofficial recipients” (Bhuyan et al., 2020, pg. 7). It is critical to note that 24% of all cyberattacks occurred within the healthcare industry in 2019, while 90% of hospitals and clinics experienced at least one data breach, and 45% experienced at least five data breaches between 2014 to 2016 (Wasserman & Wasserman, 2022). HIT systems host extensive databases of sensitive patient data that contain personally identifiable_information such as names, social security numbers, addresses, payment details, and dates of birth. Typically, financial gain is the primary motive behind 91% of data breaches because it is a lucrative black-market industry (Wasserman & Wasserman, 2022). The data available in a single electronic health record (EHR) is estimated to be a value 10 to 100 times more than stolen credit card information, and a complete set of medical records can profit $1,000 on the darknet (Bhuyan et al., 2020); Wasserman & Wasserman, 2022). The desire to foster cohesive engagement with patients across a continuum of care justifies merging EHR systems with cloud-based platforms. However, management must be just as invested in their HCO’s cybersecurity protocols as cybercriminals are in bypassing those protocols

Modern Cyberattack Methodology

Although individual cyberattacks and breaches bear a unique signature, malicious actors follow a standardized procedure to gain access to their targeted system. First, the cyber-attacker secures access to a network and identifies the scope of damage their unauthorized activity will incur on the HCO as a whole: primary infiltration will have a direct impact on patients regardless of intent, secondary infiltration indirectly affects patients and can strengthen the harm of a primary event, and tertiary infiltration has a broader focus on support systems such as electrical grids (Wasserman & Wasserman, 2022). Second, the attacker assesses the system for information and capabilities of use to their motive and typical user traffic while remaining undetected by security protocols. These observations influence the tool developed to extrapolate the chosen data and disable system capabilities, rendering it functionally useless and inaccessible to end-users.

Classification of Cyberbreach Tools

Although classifying cybersecurity threats is a challenge because of their dynamic nature, there are standard tools and methods utilized to successfully execute cyberbreaches, including the following (Bhuyan et al., 2020; Wasserman &Wasserman, 2022):

- *Denial of Service* involves overwhelming a network to the state that it cannot respond nor be accessed, so this primary infiltration technique can potentially cause physical harm to patients because it disables critical equipment such as vital monitors.
- *Privilege escalation* seeks to achieve a higher level of access to a network by converting standard user login accounts into accounts with administrative privileges.

· *Phishing*, an example of social engineering, involves the direct manipulation of an individual to digitally interact with an artifact developed by the attacker (i.e., an email) to gain access to the system.

Traditional Cybersecurity Detection and Response Measures

Ultimately, a mature IT organization is cyber resilient when they are "…able to prevent attacks, proactively prevent an attack, and quickly recover from an attack" (Abraham et al., 2019, pg. 549). In recognition of building cyber resiliency within healthcare firms, federal cybersecurity statutes have been passed, one of the most significant being the Health Insurance Portability and Accountability Act (HIPAA). This federal requirement applies to covered healthcare entities and business associates who must follow three components. The Privacy Rule protects health information on all mediums, the Security Rule sets requirements for EHRs, and the Breach Notification Rule requires entities and their associates to notify those affected by a breach of unsecured health information (*Cybersecurity in Healthcare* 2021). Unfortunately, governmental cybersecurity regulations are often ineffectual because they contain ambiguous implementation and control guidelines. For instance, HIPAA instructs non-federal HCOs to comply with a list of controls (no gold standard certifications). In contrast, federally owned health entities must apply all HIPAA guidance (Abraham et al., 2019). From a management perspective, the legal and operational complexity of ensuring hospital compliance with vague federal standards drives resource consumption and cost with an undefined return on investment. Therefore, HCO IT security budgets have remained level since 2016, and cybersecurity has decreased to 3% of the total annual IT expenditure (Leventhal, 2018). Furthermore, one-third of hospital executives that financially invest in cybersecurity solutions do so blindly (Abraham et al., 2019); 92% of healthcare data security product decisions made at the C-suite level failed to include department managers and end-users (Leventhal, 2018). The data above supports further findings that indicate only 40% of C-level executives have an in-depth understanding of their cybersecurity protocols (Abraham et al., 2019).

IT Cybersecurity Mechanisms

As previously stated, HCOs allocate a minor portion of the annual IT budget for cybersecurity programs. As a result of such financial restrictions, the traditional cyber strategy emphasizes technical end-user security per industry and organization threat assessments. End-user security focuses on the individuals interacting with systems, which includes periodically hanging passwords and segmenting hospital networks. Segmentation splits networks to prevent a single attack from compromising all essential databases (Bhuyan et al., 2020). Beneficially, database functionality is partially preserved if an attack occurs. An additional technique commonly utilized is patching software and hardware. If a bug is discovered, by the IT department, in the code of a HIT system or device, then they will release a patch that updates the targeted software to resolve the error. (Bhuyan et al., 2020). Unfortunately, patching can cause essential medical devices to become unusable because if the patch is not compatible with every software component, it disrupts device operationality. Therefore, as obsolete legacy systems continue to integrate with emerging technologies, patches will fail to provide relief.

Underfunded and understaffed IT departments become pigeonholed into adopting traditional, reactive cybersecurity measures (Bhuyan et al., 2020). Healthcare managers and administrators cannot fail to possess working knowledge of IT matters or undervalue their IT departments and staff without grave consequences. Additionally, HCOs' conventional detection and response methods are not designed to accommodate the expanding threat landscape that arrives with adopting new, interconnected, and interoperable devices.

Interoperability Within Clinical Environments

The Health Information Technology for Economic and Clinical Health Act (HITECH) triggered HIT adoption and exchange of electronic health information with the goal of every American accessing their personal EHRs (*Connecting Health…*, 2015). Interoperability is the ability of two or more HIT systems to exchange health information and use the exchanged information (*Interoperability,* 2016). Interoperability signifies that all patients and providers (both external and internal to an HCO) should be able to send, receive, find, and use EHRs in a timely and reliable manner to assist with the decision-making necessary in quality care. Moreover, interoperable HIT ecosystems support the combination of administrative and clinical data to enhance transparency and enable value-based reimbursement (*Connecting Health…,* 2015).

As of 2015, 41% of hospitals nationwide had electronic access to clinical information from outside sources, but less than half were integrating the data they received into an individual's EHR (*Connecting Health…*, 2015). In three years, a reported increase indicated that 70% of hospitals integrated data in their EHRs in 2018 (Johnson &

Pylpchuk, 2021). In order to standardize the development of advanced interoperable systems, the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare and Medicaid Services implemented separate but complementary regulations in 2020. The CMS Interoperability and Patient Access Final Regulations sought to improve claims data transparency so that patients can make informed decisions that will improve the quality of their treatments. Defined stipulations necessitate Medicare Advantage, Medicaid, Children's Health Insurance Program, and Qualified Health Plan issuers on federal exchanges to share health information in a user-friendly format through Application Programming Interfaces (Msearles, 2022). The data for adjudicated claims, laboratory results, and encounters with capitated providers must be made available through the API no later than one business day, and third-party applications may be employed to overcome software hurdles (Msearles, 2022). On the other hand, the ONC Interoperability and Information Blocking Final Regulation establishes API requirements using the Fast Healthcare Interoperability Resources (FHIR) standard (Msearles, 2022). Although the technical regulations and interoperability features appear separate from day-to-day clinical care, clinicians and management rely on interoperable HIT, such as the Internet of Medical Things (IoMT).

IoMT and Wearable Devices

The Internet of Things (IoT) consists of multiple interconnected computing devices, machines, and objects capable of transferring data within a network without human intervention (Srivastava et al., 2022). IoMT is a derivative of IoT; this healthcare-centric domain plays a crucial role in improving the precision, consistency, and throughput of connected medical devices such as in-patient vital monitors and wearable devices (Al-Muhtadi et al., 2017; Srivastava et al., 2022). Smart-based IoMT ecosystems house medical devices and software connected through the internet with third-party mobile applications to assist with real-time disease management (Srivastava et al., 2022). Wearable devices, especially, enable wireless access to healthcare data. For instance, IoMT allows physicians to monitor patients remotely with permanent pacemakers (PPMs) and implanted cardioverter defibrillators (ICDs) through cloud-based servers that provide real-time data analytics (Das et al., 2020). To best illustrate the high degree of interoperability within IoMT, Figure 1 (Srivastava et al., 2022, pg. 4) is a visual of the standard architectural overview.

[Figure 1 About Here]

The diagram begins with a data source: patient vitals acquired from a cardiac monitor. Then, the patient's data (vitals) is transmitted through multiple layers of network services. Finally, the appropriate provider receives the vitals on their device, which allows them to make a treatment decision.

IoMT Cyber Risks

Although the IoMT is an emerging technology that aligns with the healthcare industry's objective to improve interoperability, it exponentially increases the cyberattack surface. End-user actions and errors can facilitate more cyberattacks and new attack methodologies. As employees and patients continue to connect interoperable medical devices with enterprise networks, they simultaneously expose HCO networks to potential malicious activity and the individual using the device (Tarikere et al., 2021). For instance, the cyber-attacker could easily engage in primary infiltration if a patient's wearable cardiac device is connected to an infected HCO network. This attack would disrupt the device's operations, thus potentially causing physical harm to the patient if they are medically reliant on the cardiac device. The consequences of physical harm to patients due to a cyberattack are incredibly more severe than any financial damage that could occur against an HCO. Therefore, managers must consider that harnessing the advantages of IoMT only occurs there is a thorough cost-benefit analysis. The benefits of interconnected, immediate data exchanges arise from the systems' increased susceptibility to human influence and error.

Human Factors' Influence on Cybersecurity

Healthcare has a uniquely complex mission to provide quality care, so there is greater trust in employees not inappropriately disseminating patient data. Instead, the preferred organizational approach to prevent cyberattacks is technology-centric, with the belief that HIT systems can solve vulnerabilities. However, it fails to consider end-user behavior, a common mistake demonstrating that an HCO must first understand the problem and the technology itself (Pollini et al., 2021). It is apparent "…that the strength of any good information security system is in the hands of those who use it and not just the technology" (Hughes-Lartey et al., 2021). The 'people link' is the weakest component of cybersecurity. Currently, only 38% of HCOs conduct cyber training on a quarterly or biannual basis, so employees unconsciously rely on their habitual internet skills with limited guidance on security compliance (Sweeney, 2016).

According to Yeo and Banfield (2022), data breaches caused by unintentional human factors (i.e., negligence and phishing) outnumber those motivated by malicious intent. After studying 1,485 breach events between January 2015 and December 2020, they found that 141,252,797 medical records were affected. Table 1 (Yeo & Banfield, 2022) further reveals that of all the affected medical records, 73.1% resulted from breaches caused by unintentional factors. This same data appears in Figure 2 (Yeo & Banfield, 2022), which depicts the classification of the sources of EHR breaches and the frequency of occurrence during the same period. This visual indicated that 382 separate incidents were caused by unintentional negligence/carelessness. This data demonstrates that employee behavior cannot be continually monitored and controlled for an intended outcome, so a robust organizational culture is required for successful cyber procedures. The daily influence of human factors on interoperable clinical systems is evident in EHR usability.

[Table 1 and Figure 2 About Here]

EHR Usability

EHR usability is the extent to which technology is used efficiently, effectively, and satisfactorily by clinical users (Pruitt et al., 2018). A lack of EHR usability can lead to inefficiencies contributing to provider and patient dissatisfaction and patient safety risks. The ONC of Health Information Technology has requirements to promote usability, which stipulates that EHR vendors implement a user-centered design (emphasize end-user needs) and conduct usability testing of certain features at the end of the development process (Ratwani et al., 2018). A study was conducted in 2018 "… to characterize and quantify the variation in usability and the potential impact on safety that results from this variability" (Ratwani et al., 2018, pg. 1198). Two vendors were selected across four healthcare systems to measure task duration, the number of clicks needed to complete EHR tasks, and accuracy. The tested populations are all individual emergency rooms labeled Site 1A, Site 2B, Site 3B, and Site 4B. The study's results revealed that variability likely arose from local site customization of EHR systems, which directly affects end-user action. For example, researchers documented a 30% error rate from physicians at Site 3B when ordering medication, while Site 1A had no statistically significant error rate for the same task (Ratwani et al., 2018). In addition, sites 1A and 3B utilized the same vendor for their EHR systems yet had completely differing error rates. The variability in EHR-related tasks highlights the essential need for health administrators to improve software implementation and address provider error's impact on usability. IoMT and interoperability are not to be isolated from end-user influence; instead, they are intentionally designed to engage end-users. Subsequently, this will require greater organizational responsibility because appropriate digital habits within healthcare are best learned with formal training supported by technological solutions. If not adequately controlled, IoMT cybersecurity issues will continue to jeopardize healthcare access, quality, and cost.

Recommendation for Organizational Culture Change

The rise of the IoMT and other interoperable technologies have transformed how patient data impacts medical care; such technological innovation has revolutionized how HCOs improve cost, quality, and access. New risks, however, accompany these developing cyber ecosystems. Therefore, “proactive planning, defining our risk tolerance, and then managing risk according to that tolerance will decrease the angst around cybersecurity, which is the smarter approach to take, compared to how most organizations are just muddling through today” (Abraham et al., 2019, pg. 539). Although managing cybersecurity risk and building cyber resiliency within an HCO is sensitive to variable operations, all healthcare administrators must adopt a holistic cultural approach to mitigate cyberattacks. The *Healthcare Cyber Resiliency Model* (HCRM), developed from the work of Abraham et., al (2019) and Bhuyan et., al (2020), provides an organization-wide framework that leverages human and technical factors through an iterative cycle of feedback and process improvement. The HCRM is shown in Figure 3.

[Figure 3 About Here]

HCRM: Strategic Values and Budget Allocation

The first section of the HCRM necessitates HCOs to integrate their cybersecurity strategy and programs with their strategic values and budgetary priorities. A successful, viable cybersecurity program can only flourish by being recognized as a prime concern for C-suite-level executives. Drawing explicit connections between cybersecurity and quality patient care is an instrumental step that often goes unnoticed, so it must be the first step toward an organization’s cultural rebranding. In practical application, this could include revising strategic plans to promote cybersecurity and surveying employees (end-users) to audit the effectiveness of current protocols. Furthermore, it is necessary to encourage the IT department to lead a steering committee incorporating diverse viewpoints across HCO management and review all current protocols and relevant data to chart the strengths and weaknesses of the previously implemented cyber protocols.

Further, increasing the annual cybersecurity budget is a concrete step for management to recognize the value of such a program (Sweeney, 2016). Financial support is reflected by investing in additional human resources for the IT department to motivate current employees. Management cannot expect an understaffed IT department to readily accept implementing new cyber training and strategies without establishing urgency by hiring additional employees to assist with the work.

HCRM: Technological Framework

After aligning the program with an HCO's strategic values and budgetary priorities, the HRCM notes HCOs to adopt standardized technological solutions across all departments. Although a sole technological focus is ineffective in mitigating cyber risk, risk reduction only occurs with the inclusion of a practical technical approach integrated into an HCO's culture. The HCRM notes the importance of risk management. This critical process begins with understanding risk by identifying core functions of HIT systems, then valuing mitigation measures by estimating fiscal and quality outcomes of cyberattacks. Finally, concluding with communicating cybersecurity actions by increasing transparency and sharing information across all levels of the organization (Abraham et al., 2019). Risk management aids in developing device and technology safeguards (i.e., software programs). These safeguards are applied by implementing interoperable architectural standards (as shown in Figure 1) that all systems must follow. The last portion is to conduct frequent (quarterly or as-needed) end-user cyber training formulated from the architectural standards and safeguards. Overall, the technological aspect does not intend to isolate HIT physical protection from a solution-based approach intending to understand the current technology-centric policy's function (Bhuyan et al., 2020). After finalizing a unique technological approach, the HCRM notes the protocols to be carried out across all staffing levels next.

HCRM: Human Factors

The final step of the HCRM shows a circular flow of four staffing levels: executive management, middle management, lower-level management, and staff. The implementation phase is the most critical component of the model because it encompasses the human factors needed to define organizational culture. After identifying the risk management approach, architectural standards, and subsequent training, this information must have expeditious dissemination across all staffing levels. An example of such equal information sharing is the cyber training component. Completion of training modules cannot be independent of underdeveloped cybersecurity policies nor accessible by select staff. Therefore, training should be a mandatory, frequently occurring task that is interactive (i.e., simulations and real-world scenarios) and unique to the HCO’s HIT systems and vulnerabilities identified by the risk management process. After all staff and administrators complete the cyber training, cybersecurity strategies will be noticeable daily in operational activities. The final component of the HCRM includes feedback and process improvement as an output from the human factor implementation step. Feedback is collected by the interdisciplinary team responsible for overseeing cybersecurity protocols, considering the possibility of revising the program according to the strategic values and budgetary phase. If health administrators are transparent in their attempt to modify their process, then they are adequately considering their new cybersecurity approach's human and cultural aspects. In general, the intended goal of the HCRM is not to provide a specific tool but equip healthcare managers with a foundational philosophy necessary to further progress in safeguarding their emerging technologies and systems.

Conclusion

Overall, cyberattacks against healthcare institutions are increasing due to underdeveloped cybersecurity policies that fail against the expanding threat landscape. As interoperability network capabilities continue to advance, human error perpetuates cyber risks. Therefore, the HCRM is a philosophy that attempts to transition HCOs from reactive to proactive. The financial and clinical implications of using improperly secure HIT are too severe for healthcare administrators to ignore any further. Cybersecurity is not the IT department's sole issue; it never has been and never will be. Instead, cybersecurity involves the participation of every individual. HCOs must become aware of their vulnerabilities before cyberattacks; otherwise, patient safety and privacy will continue to be jeopardized.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. Healthcare Industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2017). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal*, *25*(2), 315–329. https://doi.org/10.1177/1460458217706184

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Healthcare Cybersecurity from reactive to proactive: Current status and future recommendations. *Journal of Medical Systems*, *44*(5). https://doi.org/10.1007/s10916-019-1507-y

Das, S., Siroky, G. P., Lee, S., Mehta, D., & Surit, R. (2020). Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm, 18*(3), 473–481. https://doi.org/https://doi.org/10.1016/j.hrthm.2020.10.009

Editor. (n.d.). *Cyber attack - glossary: CSRC*. Computer Security Resource Center. Retrieved November 8, 2022, from https://csrc.nist.gov/glossary/term/Cyber_Attack

Epalm. (2021, December 16). *Cybersecurity in Healthcare*. HIMSS. Retrieved November 17, 2022, from https://www.himss.org/resources/cybersecurity-healthcare

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's internet of things. *Heliyon*, *7*(3). https://doi.org/10.1016/j.heliyon.2021.e06522

Information Technology Laboratory . (n.d.). *Cyber attack - glossary: CSRC*. Computer Security Resource Center. Retrieved November 8, 2022, from https://csrc.nist.gov/glossary/term/Cyber_Attack

Interoperability. Federal Communications Commission. (2016, October 24). Retrieved November 17, 2022, from https://www.fcc.gov/general/interoperability#:~:text=The%20Institute%20of%20Electrical%20and%20Electronic%20Engineers%20%28IEEE%29,to%20use%20the%20information%20that%20has%20been%20exchanged.%22

Johnson, C., & Pylpchuk, Y. (2021). (rep.). *Use of Certified Health IT and Methods to Enable Interoperability by U.S. Non-Federal Acute Care Hospitals, 2019*. ONC. Retrieved December 3, 2022, from https://www.healthit.gov/data/data-briefs/use-certified-health-it-and-methods-enable-interoperability-us-non-federal-acute.

Leventhal , R. (2018, May 16). *Cyber attacks increase as it security budgeting remains static, report ...* Healthcare Innovation. Retrieved November 17, 2022, from https://www.hcinnovationgroup.com/cybersecurity/news/13030218/cyber-attacks-increase-as-it-security-budgeting-remains-static-report-finds

Msearles. (2022, May 31). *Final CMS interoperability regulation: What you need to know*. HIMSS. Retrieved October 12, 2022, from https://www.himss.org/news/final-cms-interoperability-regulation-what-you-need-know

The Office of the National Coordinator for Health Information Technology, Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap (2015). The Office of the National Coordinator for Health Information Technology. Retrieved October 12, 2022, from https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pruitt, Z. M., Howe, J. L., Hettinger, A. Z., & Ratwani, R. M. (2021). Emergency Physician Perceptions of Electronic Health Record Usability and Safety. *Journal of patient safety*, *17*(8), e983–e987. https://doi.org/10.1097/PTS.0000000000000849

Ratwani, R. M., Savage, E., Will, A., Arnold, R., Khairat, S., Miller, K., Fairbanks, R. J., Hodgkins, M., & Hettinger, A. Z. (2018). A usability and safety analysis of electronic health records: A multi-center study. *Journal of the American Medical Informatics Association*, *25*(9), 1197–1201. https://doi.org/10.1093/jamia/ocy088

Srivastava, J., Routray, S., Ahmad, S., & Waris, M. M. (2022). Internet of medical things (IoMT)-based smart healthcare system: Trends and progress. *Computational Intelligence and Neuroscience*, vol. 2022, 1–17. https://doi.org/10.1155/2022/7218113

Sweeney, B. (2016, September 13). Cybersecurity is every executive's job. Harvard Business Review. Available at https://hbr. org/2016/09/cybersecurity-is-every-executives-job

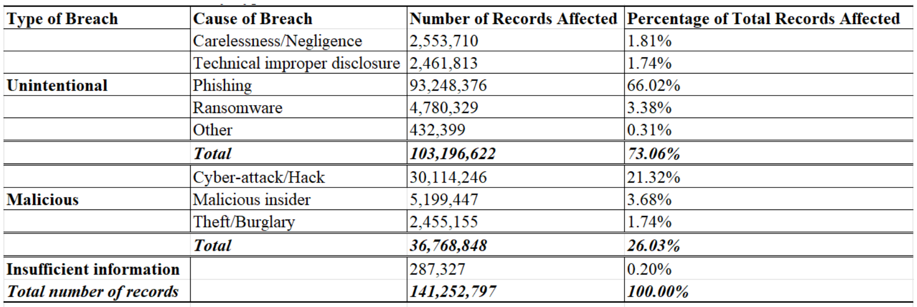
Tarikere, S., Donner, I., & Woods, D. (2021). Diagnosing a healthcare cybersecurity crisis: The impact of IOMT advancements and 5G. *Business Horizons*, *64*(6), 799–807. https://doi.org/10.1016/j.bushor.2021.07.015

Wasserman, L. & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*. https://doi.org/10.3389/fdgth.2022.862221

Yeo, L. H. & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, *19*(2), 92–101.

Table 1

Number of Affected Records by Type and Source of Breach

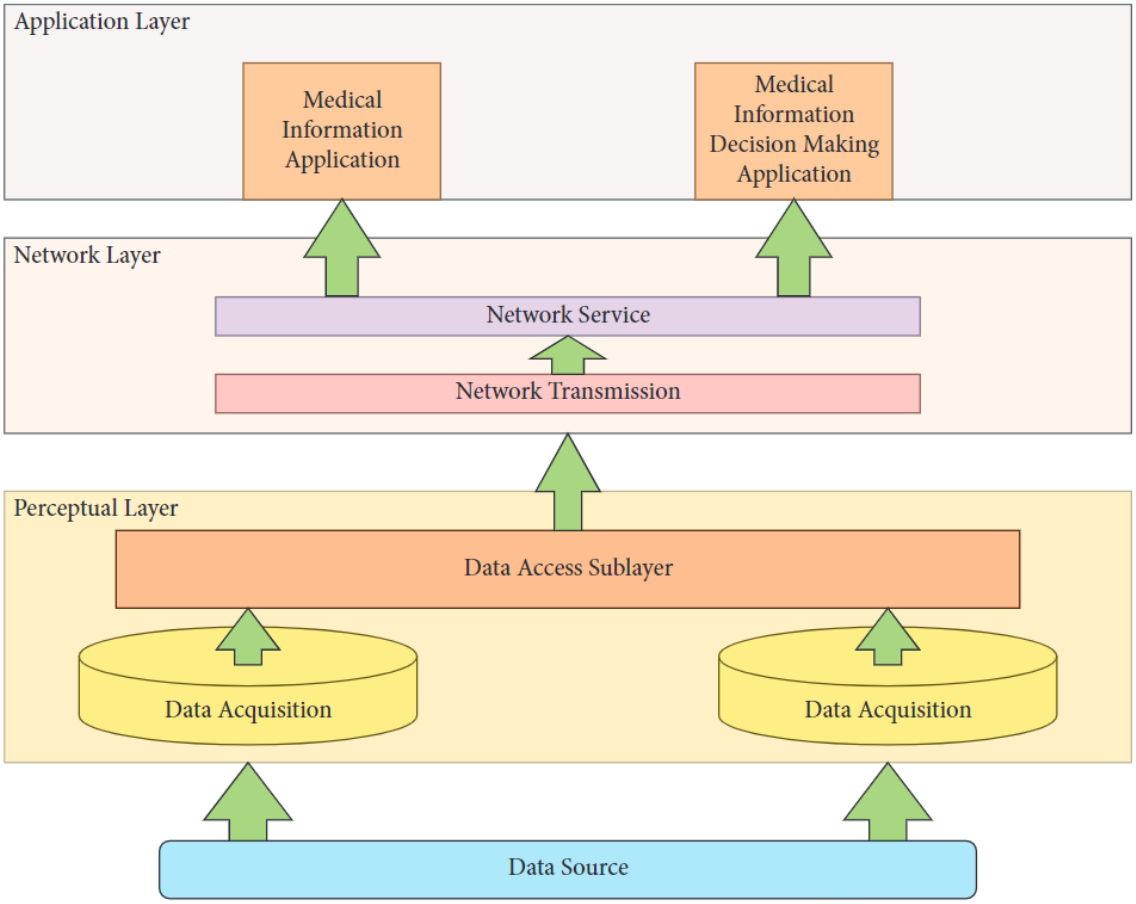


Type of Breach	**Cause of Breach**	**Number of Records Affected**	**Percentage of Total Records Affected**
	Carelessness/Negligence	2,553,710	1.81%
	Technical improper disclosure	2,461,813	1.74%
Unintentional	Phishing	93,248,376	66.02%
	Ransomware	4,780,329	3.38%
	Other	432,399	0.31%
	Total	***103,196,622***	***73.06%***
	Cyber-attack/Hack	30,114,246	21.32%
Malicious	Malicious insider	5,199,447	3.68%
	Theft/Burglary	2,455,155	1.74%
	Total	***36,768,848***	***26.03%***
Insufficient information		287,327	0.20%
Total number of records		***141,252,797***	***100.00%***

Note: Reprinted from “Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis.” By Yeo, L. H. & Banfield, J., 2022, *Perspectives in Health Information Management*, *19*(2), Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/.

Figure 1

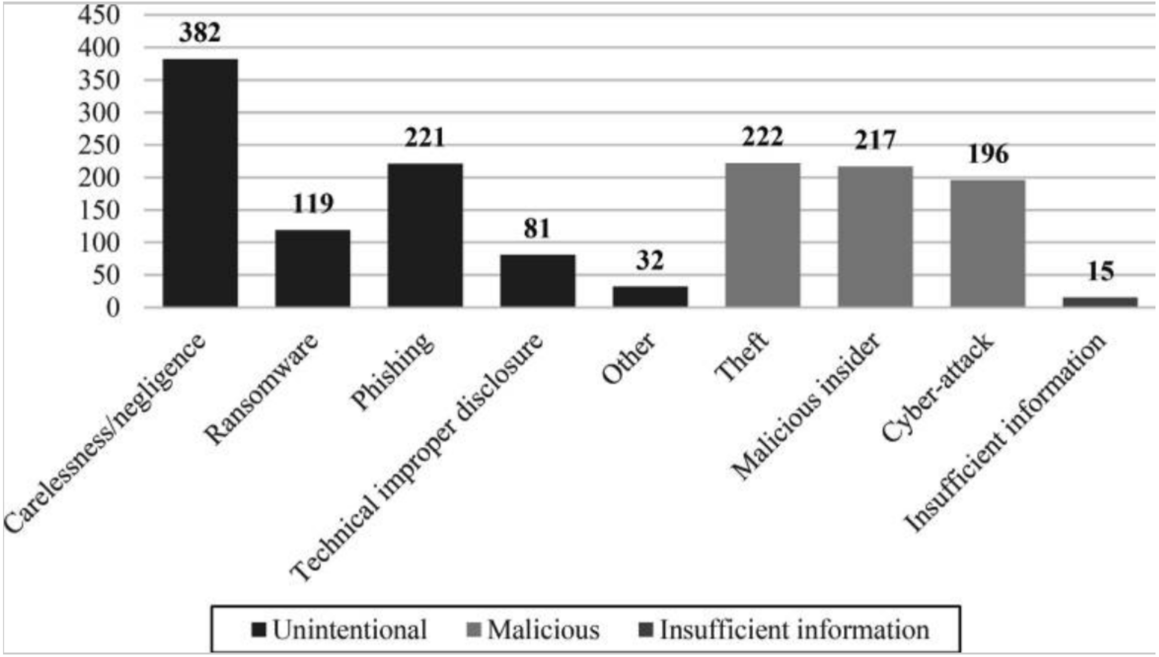
IoMT Architectural Overview



Note: Reprinted from "Internet of medical things (IoMT)-based smart healthcare system: Trends and progress" by Srivastava, J., Routray, S., Ahmad, S., & Waris, M. M., 2022, *Computational Intelligence and Neuroscience*, vo. 2022, Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9308524/.

Figure 2

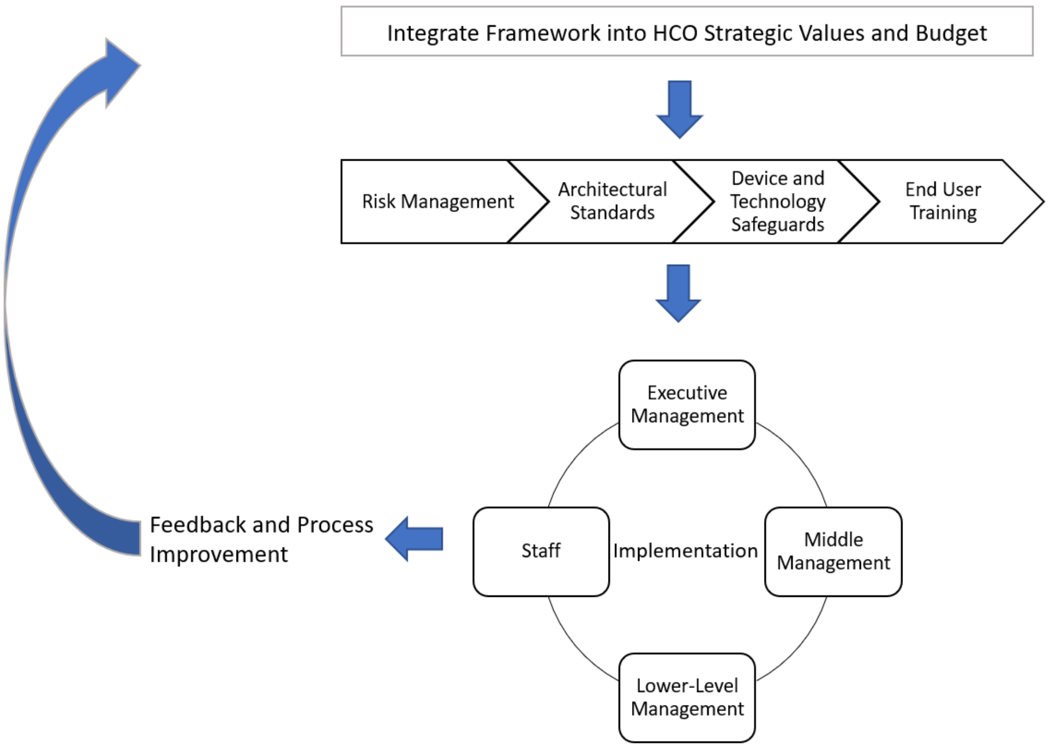
Sources and Frequencies of EHR Breaches



Note: Reprinted from “Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis,” by Yeo, L. H. & Banfield, J., 2022, *Perspectives in Health Information Management*, *19*(2), 92–101, retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/.

Figure 3

Healthcare Cyber Resiliency Model



Note: The proposed model was developed from concepts outlined in "Muddling through cybersecurity: Insights from the U.S. Healthcare Industry" by Abraham, C., Chatterjee, D., & Sims, R. R., 2019, *Business Horizons*, *62*(4), 539–548, and in "Transforming Healthcare Cybersecurity from reactive to proactive: Current status and future recommendations" by Bhuyan, S. S., et al., 2020, *Journal of Medical Systems*, *44*(5) retrieved from https://doi.org/10.1007/s10916-019-1507-y.