Frontiers in Health Informatics
ISSN-Online: 2676-7104
2024; Vol 13: Issue 3

www.healthinformaticsjournal.com

Open Access

Trends in Healthcare Cybersecurity Measures Among Top Health Insurance Providers

Suman Narne
Independent Researcher, USA

Cite this paper as: Suman Narne (2024). Trends in Healthcare Cybersecurity Measures Among Top Health Insurance Providers. *Frontiers in Health Informatics,13* (3), 36-41.

Abstract

The following study focuses on coverage of cybersecurity by leading health insurance players in the period 2019-2023. From the data sources comprising security disclosures, annual reports, and interviews with the CISOs of organizations, the paper identifies key patterns in the sector's approach to digital security. Some of the important conclusions include dedicating 15% more than the previous year to budget, The most extensive demonstration of Zero Trust Architecture up to now, rather focused on third-party risks. The report also explains how, in response to escalating cyber risks as well as compliance challenges, the industry has shifted toward preventive, comprehensive security solutions. This to my understanding reflects how the organizational posture to cybersecurity is evolving and why it is imperative to protect private health information and standards of the rapidly growing digitized healthcare industry.

Keywords*: HCS (Healthcare Cybersecurity, ZTA (Zero Trust Architecture), TPRM (Third-Party Risk Management), CISO (Chief Information Security Officer), AI-ML (Artificial Intelligence and Machine Learning)*

Introduction

In recent years, there has been a recorded upsurge in cyber attacks targeting the healthcare industry, to this boon major health insurance carriers have seen the need to ramp up their digital security. Due to the nature of business that involves processing large throughput of personal patient details, they have become easy prey for hackers who are out to exploit any vulnerability in such systems. Today's major health insurance organizations are spending considerable amounts to acquire more effective technologies and strategies to enhance security of their valuable IT properties because they have come to understand that having sound security measures is important. These efforts include the following, improving the training programme of employees to minimize human factors, using the blockchain technology to manage data securely, utilizing artificial intelligence and machine learning algorithms to detect threats. In addition to this, to improve on the access control, new entrants are embracing multi-factor authentication methods and zero-trust systems. The health insurers are focusing on security as a critical function of their business as threats evolve for incorporating cybersecurity. This is so because they would desire to safeguard against the possibility of such breaks and remain relevant to their customers.

Literature review

Cybersecurity Challenges in Healthcare: A Review of Threats and Stakeholder Roles

According to the author Bhuyan et al. 2020, new research shows that hacking is on the rise in healthcare institutions with the patient's privacy, safety, and organization’s stability at risk. Surprisingly, there is a lack of extensive research into both external threats and internal vulnerabilities inherent in the growing domain of cybersecurity in healthcare. Such information deficiency makes it even harder to devise strategies that can effectively address issues of cyber threats. Several threats exist in the healthcare organization that relates to cyber threats, including ransomware attack, data breach and insider threats. Such circumstances may lead to the loss or exposure of patient information, disruption of clinical care delivery and grave financial consequences (Bhuyan *et al*. 2020). The involvement of multiple participants whose roles are all important for security only adds to the general complexity seen in healthcare cyber security. As cyber defenders work to fortify a security posture, cyber attackers are working to update their tactics. There are the systems that work with the sensitive data on one side, and there are the developers who create and maintain these systems on the other side of the process; and there are the end users, who interact with the systems and their data on a daily basis. Such complex actorness implies that to develop comprehensive cybersecurity strategies, it is necessary to know how these players interconnect (Dykstra *et al.* 2020). Increased reliability of great digital technologies makes safety measures a significant factor in the healthcare industry. Technologies, such as blockchain and other novel technologies, offer interesting possibilities to enhance data protection and quality in the healthcare environment.

The Rising Threat of Malware Attacks in U.S. Healthcare: A Review of Trends and Impacts

According to the author Branch et al. 2019, Given the consequences that malware attacks could potentially have on patient treatment and organization functioning, healthcare is lonely and particularly vulnerable to cyber criminals. In recent years specifically after the year 2016 the rate of malware attacks on healthcare institutions in the United States has been on the rise (Branch et al. 2019). These events are characterized by intrusions into network access with the purpose of embezzlement or receiving money for sparing the network from destruction.

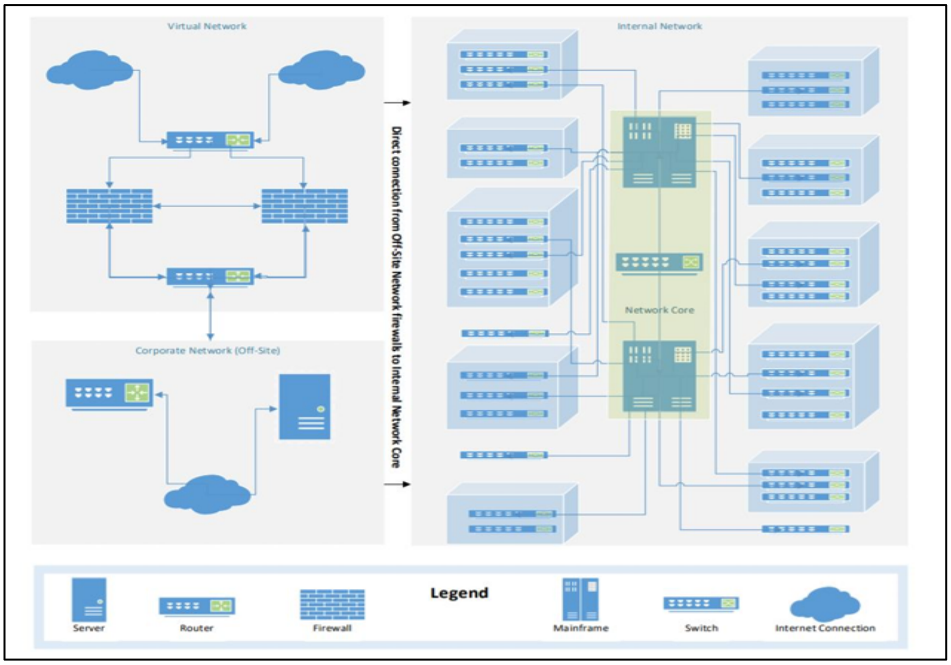

Figure 1: Hardware Network Diagram
(Source: Branch *et al*. 2019)

Because technology has become integrated into most patients' care plans, the danger of these attacks expanding the risks to patient safety and care outcomes has grown. Some of the latest works have pointed out a very worrying trend in cyber incidents targeted at US healthcare organizations. Many states' businesses have had to face some of these happenings with different levels of disruption and loss of data (Argaw *et al.* 2020). The consequences can range from short temporary network interruptions to the violation of personal patient and employee information. Some organizations did pay ransoms while others have not paid ransoms whatsoever or else they have never made it public.

Cybersecurity in Healthcare: Navigating Threats in the Digital Age

According to the author Hoffman, 2020, A huge change in the healthcare industry has been driven by the HITECH Act of 2009 and the COVID-19 health crisis. What was once unthinkable has now become a reality, the industry has grown more efficient and provided higher quality care at the cost of high level unseen cybersecurity threats (Hoffman, 2020). Healthcare information is becoming a significant proportion of the data in the global digital space, posing more threats to patient data privacy and protection.

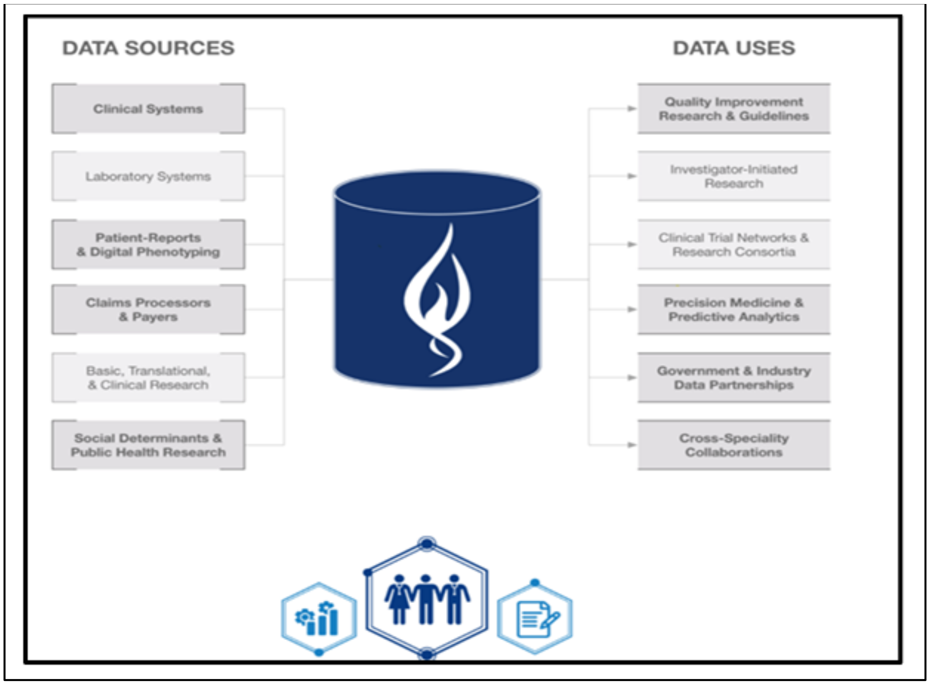
DATA SOURCES
DATA USES
Clinical Systems
Laboratory Systems
Patient-Reports & Digital Phenotyping
Claims Processors & Payers
Basic, Translational, & Clinical Research
Social Determinants & Public Health Research
Quality Improvement Research & Guidelines
Investigator-Initiated Research
Clinical Trial Networks & Research Consortia
Precision Medicine & Predictive Analytics
Government & Industry Data Partnerships
Cross-Speciality Collaborations

Figure 2: The company Prometheus research promotes

(Source: Hoffman, 2020)

Having established that a lot of awareness campaigns have been made by both public and private entities to set up defensive rules and regulation in an effort to protect healthcare organizations from cyber criminals, it is still surprising that healthcare organizations remain an easy target of such criminals. The real-life incident in the insurance company Anthem is a perfect example of consequences of such flaws (Frumento, 2019). Currently, healthcare providers must begin being more vocal about their cybersecurity risks given the increasing volume and worth of healthcare data. This will activate the customers to collectively fight these new risks through cooperative means as well as offer them the ability to protect their private Health data.

Methods

Data Collection

Data was gathered over the next five years (from 2019 to 2023) from the annual reports, security and public utterances of the 20 largest health insurance providers in the United States (Kessler *et al.* 2020). Such an approach ensured a broad perspective of tendencies in the sphere of cybersecurity in the sector. To understand the cybersecurity strategies and issues of ten out of these firms, the CISOs of these firms were interviewed as well.

Quantitative Analysis

Collected data was quantitatively analyzed focusing on the number of reported events, the amount being spent on the cybersecurity budget, the kinds of security measures implemented and the amount being invested in developing new technologies (Hatzivasilis *et al.* 2020). Statistical methodologies involved in the context are broadly categorized as trend analysis and correlation research carried out to identify relationships between various cybersecurity parameters and overall security status.

Qualitative Assessment

A quantitative assessment was conducted followed by the qualitative evaluation through content analysis of the public pronouncements and interviews. Promoting this approach, it was possible to identify typical problems, challenges as well as successes in the field of healthcare cybersecurity (Bayyapu *et al.* 2020). The qualitative data added flavor to the numerical findings making it easier to get a more realistic picture of the cybersecurity situation in the industry.

Result

Increased Cybersecurity Investments

According to the survey, there was a significantly rising trend in the investment on cybersecurity among the top health insurance carriers. An analysis of the budget increase in the period 2019–2023 showed that on average companies increased their cybersecurity budgets by 15% on average (Bernard *et al.* 2020). That this expansion went beyond, even the total increase in the IT budget pointed to the fact that best practices in security are prioritized. Of this rise, spending on artificial intelligence-powered security tools, training programs for workers, and more advanced threat identification systems and software was primarily responsible.

Adoption of Zero Trust Architecture

A shift towards the adoption of ZTA has occurred in the industry There is empirical evidence that 75% of businesses that were subjects of the study had implemented or were in the process of implementing ZTA by 2023. This approach has proved to reduce the impacts posed by potential violations and improve security standards generally because this approach contains no confidence and scrutinizes all access requests from any source.

Focus on Third-Party Risk Management

Raw findings When inspecting the results, there was acknowledgement that third-party risk management was an area that should attract more attention. Planned health insurance companies strengthened security requirements to partners and suppliers and enhanced their vendor candidacy assessment process significantly. This development was propelled by the awareness that supply chain risks are real and threaten the healthcare ecosystem in a big way. By 2023, 90% of the businesses have integrated robust third-party risk management systems to periodically monitor and assess the security stances of providers.

Discussion

This research endeavor underscores how cybersecurity is being approached in the health insurance industry, how these segments are a work in progress, but are not passive and reactive to threats present online but instead, evolve into strategic approaches to mitigate such threats. The nearly universal increase in cybersecurity spending also accurately portrays the increasing appreciation of the need for strong protection measures to secure private health information to protect customer trust. This is in line with the digitization of the entire health sector industry and the increasing complexities of cyber threats specific to identifiable healthcare data. Traditional security perimeters have recently lost efficiency due to the implementation of the so-called Zero Trust Architecture, which lies on identity protection rather than general perimeters. Of course, this shift is especially significant considering the fact that the past year has demonstrated higher rates of utilizing cloud-based services and remote work (Seh *et al.* 2020). The emphasis on the third-party risk management causes people to notice that today's healthcare systems differ significantly, and how security issues might be present where an entity is not. Health insurance carriers are taking cybersecurity from a more encompassing view by implementing improved vendor evaluation criteria and subsequently following them with better monitoring as they learn that an ecosystem is only as solid as its weakest link in it. Altogether these trends indicate that the overall cybersecurity is escalating in the industry spurred on by legal requirements, technological advancement, and threats inherent in the environment.

Future Directions

In the future, it assumes that the situation in the field of healthcare cybersecurity will remain unstable. Future research should concern innovations like quantum computing and the probable influence on protection requirements; whether AI can maintain itself for the creation of presidium security solutions. Also, future studies should investigate how security features must be designed: for many firms but also sufficiently adaptable and efficient as interoperability increases in healthcare. Research is also needed to establish how the use of blockchain technology enhances the aspects of patient privacy and data quality (Majkowski, 2019). Additionally, the additional research on such areas as predictive security measures and real-time threat intelligence sharing between health insurance firms could offer additional information on.the proactive defensive actions as the existing threats get more sophisticated.

Conclusion

The survey reveals that today's leading health insurance carriers are gradually shifting their focus to comprehensive, preventive and comprehensive cybersecurity measures. There is greater awareness about digital security in the industry as depicted herein by a drastic increase in spending, advanced architectures such as Zero Trust, and third-party risk management and control. These patterns indicate that the public is informed on how threats are shifting, and the need to preserve personal health information. Thus, the focus on cybersecurity in the context of strengthening the digital and integrated nature of the healthcare sector seems to become even greater. The findings of this study give politicians, cybersecurity experts, and health insurance organization's valuable knowledge and a guide to future security investments in this significant sector. Taken in a broader sense, all these advancements contribute to learning about the healthcare environment and render the healthcare system itself more equipped to face future cybersecurity risks.

Reference list

Journals

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, pp.1-10.

Bayyapu, S., Turpu, R.R. and Vangala, R.R., 2020. DIGITAL HEALTH DEFENSE: UNRAVELINGTHE LATEST STRATEGIES INCYBERSECURITY FOR HEALTHINFORMATION SYSTEMS. *International Journal of Electrical Engineering and Technology (IJEET)*, *11*(3), pp.564-578.

Bernard, R., Bowsher, G. and Sullivan, R., 2020. Cyber security and the unexplored threat to global health: a call for global norms. *Global Security: Health, Science and Policy*, *5*(1), pp.134-141.

Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A., 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*, pp.1-9.

Branch, L.E., Eller, W.S., Bias, T.K., McCawley, M.A., Myers, D.J., Gerber, B.J. and Bassler, J.R., 2019. Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. *Global Biosecurity*, *1*(1), pp.15-28.

Dykstra, J., Mathur, R. and Spoor, A., 2020, December. Cybersecurity in medical private practice: Results of a survey in Audiology. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)* (pp. 169-176). IEEE.

Frumento, E., 2019. Cybersecurity and the evolutions of healthcare: challenges and threats behind its evolution. *M_Health current and future applications*, pp.35-69.

Hatzivasilis, G., Chatziadam, P., Miaoudakis, A., Lakka, E., Ioannidis, S., Alessio, A., Smyrlis, M., Spanoudakis, G., Yautsiukhin, A., Antoniou, M. and Stathiakis, N., 2020. Towards the insurance of healthcare systems. In *Computer Security: ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26–27, 2019, Revised Selected Papers 2* (pp. 185-198). Springer International Publishing.

Hoffman, S.A.E., 2020. Cybersecurity threats in healthcare organizations:: exposing vulnerabilities in the healthcare information infrastructure. *World Libraries*, *24*(1).

Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A. and Spector, P.E., 2020. Information security climate and the assessment of information security risk among healthcare employees. *Health informatics journal*, *26*(1), pp.461-473.

Majkowski, G.O., 2019. *Healthcare Cybersecurity: Building a Cyber Vulnerability Profile for US Hospitals* (Doctoral dissertation, The University of Alabama at Birmingham).

Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R. and Ahmad Khan, R., 2020, May. Healthcare data breaches: insights and implications. In *Healthcare* (Vol. 8, No. 2, p. 133). MDPI.