Scientific Research Publishing

Journal of Information Security, 2025, 16(3), 437-445
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Ransomware Attacks: Evidence of Network Security Vulnerability in Work-from-Home Setups during the COVID-19 Pandemic Lockdown

Mohammed Mohammed Raoof[1], Rafeeq Al-Hashemi[2]

[1]Center for Information Systems & Technology, Claremont Graduate University, Claremont, USA
[2]Computer Science Department, Illinois Central College, East Peoria, USA
Email: mohammedraoofphd@gmail.com

How to cite this paper: Mohammed Raoof, M. and Al-Hashemi, R. (2025) Ransomware Attacks: Evidence of Network Security Vulnerability in Work-from-Home Setups during the COVID-19 Pandemic Lockdown. *Journal of Information Security*, **16**, 437-445.
https://doi.org/10.4236/jis.2025.163022

Received: May 27, 2025
Accepted: July 26, 2025
Published: July 29, 2025

Abstract

Ransomware attacks are common in the United States (US) healthcare industry, causing data breaches. They can also cause many harmful effects, including reputation loss, operational downtime, legal liabilities, financial loss, the possibility of losing the business, and even risks to the lives of patients who use Internet of Things (IoT) medical devices. In addition, ransomware attacks are risky for patients' lives who utilize medical computer systems in inpatient facilities, such as Long-Term Acute Care Hospitals (LTACHs) and Skilled Nursing Facilities (SNFs). However, this study uses the phenomenological research method to analyze the ransomware attacks on US healthcare practitioners represented by US healthcare entities (A Healthcare Provider, A Health Plan, and A Healthcare Clearinghouse). The authors retrieved the US healthcare breaches from 2014 to 2024, listed in the US Department of Health and Human Services, Office for Civil Rights report. Moreover, the authors employed data limitations to enforce the validity of the study. The findings show that ransomware attacks occurred during the COVID-19 pandemic lockdown period, particularly during the common practice of work-from-home. This study concluded that network security is a severe breaching factor for work-from-home practice in healthcare settings and suggested the need to enforce the implementation of robust cybersecurity measures, such as the NIST SP 800-66 R2 security standard for remote working, and increase the security awareness of work-from-home worker based on Artificial Intelligence (AI) to help mitigate the potential risk of ransomware attacks.

Keywords

Internet of Things (IoT), Artificial Intelligence (AI), SP 800-66, COVID-19

Pandemic Data Breaches, Work-From-Home, Long-Term Acute Care Hospitals (LTACHs), Skilled Nursing Facilities (SNFs), Acute Care Hospitals, Rehabilitation Hospitals, Hospice Care Centers

1. Introduction

Ransomware is a blend of the words "ransom" and "software" [1]. A medical researcher, Dr. Joseph Popp, created the first ransomware, the "AIDS Trojan," in 1989 by distributing 2000 infected floppy disks to his fellow researchers who attended a conference for the World Health Organization (WHO) on AIDS, demanding payment to unlock users' computers [2]. With the internet's New Age, any individuals and businesses connected to the internet are at risk for ransomware attacks. However, ransomware is a form of malware that emerged in 2013 [3]. The primary purpose of ransomware criminals is to make an easy income from the victims of ransomware attacks. Technically, this type of malware locks victims' computers and forces them to pay a ransom (e.g., money or cryptocurrency, such as Bitcoin). Once the ransomware criminals receive the ransom, the victims' computers are unlocked, and their data is retrieved.

Typically, ransomware criminals use various techniques to attack the victims, such as encrypting the valuable files of the victims' machines, asking for ransom, and decrypting these files after the ransom is paid [4], but paying the ransom may be illegal [5]. However, ransomware is not limited to one type. There are several types of ransomware, including Cerber, CryptoLocker, CryptXXX, CryptoWall, Locky, NoobCrypt, NotPetya, Nyetya, SamSam, BadRabbit, and WannaCry [6] [7]. Moreover, ransomware is one of the various attacks on the Internet of Things (IoT) devices [8]. Atadoga, Omaghomi [9] noted, "IoT technologies have significant applications in the healthcare industry, revolutionizing patient care and healthcare management. Wearable health monitors, including fitness trackers and smartwatches, have become indispensable tools for individuals seeking to monitor their vital signs, sleep patterns, and physical activity." That said, ransomware attacks on IoT devices pose a likely risk to patients who use IoT devices for medical treatment. In addition, ransomware attacks are risky for patients' lives in inpatient facilities, such as acute care hospitals, rehabilitation hospitals, hospice care centers, Long-Term Acute Care Hospitals (LTACHs), and Skilled Nursing Facilities (SNFs). These inpatient facilities' computer systems, including the medical devices used by patients, are connected to their internal networks, enabling ransomware criminals to disrupt the operations of their medical computer systems.

What would have happened if the ransom had not been paid? Ransomware has harmful consequences if the ransom is not paid to the criminals. The consequences of ransomware attacks harm individuals in various ways, including losing personal documents, such as any documents saved on the victims' computers that

include sensitive personal information. In contrast, ransomware attacks are more harmful to businesses because they cause operational downtime, legal liabilities, financial losses, and reputational damage, which applies to breaches in the United States (US) healthcare industry; Raoof [10] documented the outcomes of US healthcare breaches, "resulting in financial loss, reputation loss, and the possibility of losing the business."

Related Work

Spence, Niharika Bhardwaj [11] conducted a literature review focusing on ransomware attacks in healthcare facilities; their study was limited to sources published in English from 2005 to 2017. They addressed the financial costs of surviving ransomware attacks, reputation damage leading to loss of future business, and techniques for protecting against Ransomware, such as employees' awareness and data backup. Moreover, Neprash, McGlave [12] questioned how often healthcare delivery organizations encounter ransomware attacks and how the attacks' characteristics change over time. They concluded that the current reporting efforts of Ransomware attacks provide limited information. Their findings acknowledged that ransomware attacks disrupt care delivery and jeopardize data integrity. In another study, Dameff, Tully [13] concluded the potential medical risks that may occur due to ransomware attacks on patients with acute stroke conditions inside hospitals. None of the papers cited in the related work section is directly relevant to the focus of our study.

However, this paper investigates the ransomware attacks in US healthcare over the last ten years, from 2014 to 2024. Specifically, our study focuses on identifying which covered entity was highly targeted by ransomware criminals and also defines the common types of security gaps for this type of attack in the US healthcare industry. In addition, this paper contributes to increasing awareness of security gap types in the covered entities. Our findings will help healthcare practitioners, engineers, and security developers better protect patient data against ransomware attacks, which will help reduce future ransomware attacks in the US healthcare industry.

2. Methodology

In this study, the authors used the qualitative phenomenological research method. The purpose of the phenomenology approach is "to describe the essence of a phenomenon by exploring it from the perspective of those who experienced it" [14]. US healthcare practitioners who are represented by US healthcare entities (A Healthcare Provider, A Health Plan, and A Healthcare Clearinghouse). According to the breach report of the U.S. Department of Health and Human Services - Office for Civil Rights [15], the US healthcare entities have experienced ransomware attacks. Hence, we have not conducted interviews to collect primary data. We intended to use the secondary data in our study because it included documented Ransomware attacks experienced by the US healthcare industry.

2.1. Data Collection

This paper focuses on the US healthcare breaches listed in the U.S. Department of Health and Human Services-Office for Civil Rights [15]. The authors retrieved the archived resolved breach reports over the last ten years, from July 24, 2014, to July 24, 2024. The retrieved data were collected on July 24, 2024. These data are available to the public, U.S. Department of Health and Human Services-Office for Civil Rights [15] documented, "As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary."

2.2. Data Limitation

To ensure the validity of the data in the archived resolved breach reports of the U.S. Department of Health and Human Services - Office for Civil Rights [15], the researchers excluded the mixed Location of Breach categories when they retrieved the data in the resolved breach reports.

2.3. Research Question

Given the ransomware attacks in the US healthcare industry listed in the US Department of Health and Human Services, Office for Civil Rights report. Particularly, from 2014 to 2024, this study attempts to answer the following questions:

- What covered entity has the highest number of ransomware attacks?
- What common security gaps in the US healthcare industry are used by ransomware criminals?

3. Analysis

Boadu [16] discussed the importance of using theme analysis from a lived experience in the context of phenomenological research. Hence, the researchers of this study relied on theme analysis, specifically represented the theme analysis by tables; they used Microsoft Excel to navigate the US Department of Health and Human Services, Office for Civil Rights archived report, which includes the field of "Web Description" that describes additional information about the experiences of each breach. However, the additional information in the "Web Description" field includes words that describe the type of attack (e.g., ransom or ransomware).

The authors looked in the "Web Description" field for the keyword "ransom" and showed the results of all the ransomware attacks from 2014 to 2024. Although the analysis involved counting the keyword "ransom" and organizing results in tables below, it adheres to thematic analysis standards. Thematic interpretation was guided by experienced US healthcare practitioners who had experienced the ransomware attacks, ensuring analytical depth beyond simple frequency [17].

The filtration was formulated only to show the results for US healthcare entities (A Healthcare Provider, A Health Plan, and A Healthcare Clearinghouse). The researchers of this study represented each healthcare entity by a theme.

In addition, the researchers have also used charts to enhance the interpretation of data.

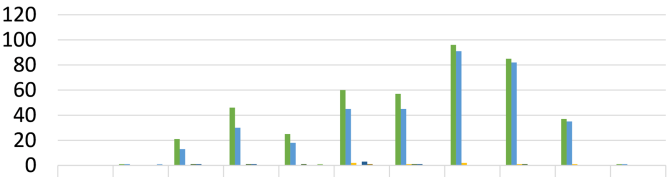
4. Findings

The results show 469 ransomware breaches out of 4312 total breaches. Moreover, 38,250,199 individuals were affected by these 469 breaches. Table 1 shows the details of these numbers with percentages.

Table 1. Categorized covered entities based on the number of breaches and affected individuals.

Theme Represented by A Healthcare Entity	Number of Breaches	Number of Breaches (Percentage %)	Number of Affected Individuals	Number of Affected Individuals (Percentage %)
Healthcare Provider	429	91.47%	37,334,582	97.61%
Health Plan	40	8.53%	915,617	2.39%
Healthcare Clearinghouse	0	0	0	0
	469	100%	38,250,199	100%

In addition, this study calculated the number of breaches categorized by a unique Location of Breach categories (Desktop Computer, Paper/File, Other, Electronic Medical Record, Email, Laptop, and Network Server), submitted annually between 2014 and 2024 for healthcare provider and health plan entities. No ransomware attacks occurred against the Healthcare Clearinghouse entity during that period. However, Figure 1 shows the findings for the healthcare provider entity as follows:



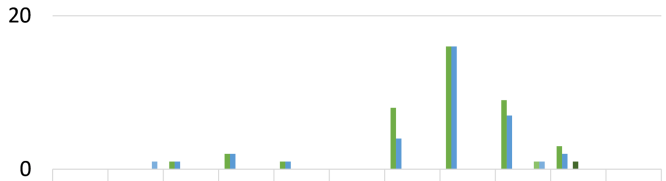
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Breach Submission Date	0	1	21	46	25	60	57	96	85	37	1
Network Server	0	1	13	30	18	45	45	91	82	35	1
Electronic Medical Record	0	0	0	0	0	2	1	2	1	1	0
Email	0	0	1	1	1	0	1	0	1	0	0
Desktop Computer	0	0	1	1	0	3	1	0	0	0	0
Laptop	0	0	0	0	0	1	0	0	0	0	0
Paper/Films	0	0	0	0	1	0	0	0	0	0	0
Other	0	1	0	0	0	0	0	0	0	0	

Figure 1. Number of submitted breaches for healthcare provider entity with a unique location of breach categories.

Their peak experience of ransomware attacks was 60 in 2019, 57 in 2020, 96 in

2021, 85 in 2022, and 37 in 2023. Moreover, the Network Server category shows the highest peak among these years, as a common security gap that ransomware criminals use.

Figure 2 shows the findings for the Health Plan Entity. Their peak experience of ransomware attacks was 0 in 2019, 8 in 2020, 16 in 2021, 9 in 2022, and 3 in 2023. The Network Server category also shows the highest peak among the following years: 2020, 2021, and 2023, as a common security gap that ransomware criminals use.



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Breach Submission Date	0	0	1	2	1	0	8	16	9	3	0
Network Server	0	0	1	2	1	0	4	16	7	2	0
Electronic Medical Record	0	0	0	0	0	0	0	0	0	0	0
Email	0	0	0	0	0	0	0	0	0	1	0
Desktop Computer	0	0	0	0	0	0	0	0	0	0	0
Laptop	0	0	0	0	0	0	0	0	0	0	0
Paper/Films	0	0	0	0	0	0	0	0	1	0	0
Other	0	1	0	0	0	0	0	0	1	0	0

Figure 2. Number of submitted breaches for health plan entity with a unique location of breach categories.

5. Discussion

As shown in Table 1, it answered the first research question. Healthcare Providers have the highest number of breaches and affected individuals, followed by the Health Plan entity, while there is no Healthcare Clearinghouse. Figure 1 and Figure 2 show the findings for Healthcare Provider Health Plan Entities. Both findings visualized their high peak experience of ransomware attacks during the COVID-19 pandemic lockdown period, particularly during the following years: 2019, 2020, 2021, 2022, and 2023. Both figures also show network servers as the highest security gap for ransomware criminals, which answers the second research question. However, remote working was a well-known phenomenon as a common business practice during the COVID-19 pandemic [18] [19]. Typically, remote working occurs outside healthcare entities, such as at home via a home network (e.g., Wireless Fidelity (WiFi) enables devices like smartphones, tablets, and laptops), where the security setup differs from that of healthcare entities.

According to the findings of this study, the researchers concluded that remote work from home in healthcare entities is likely risky for network security breaches

unless it is well supported with robust network security mechanisms, such as enforcing the implementation of the National Institute of Standards and Technology (NIST), including NIST Special Publication (SP) 800-66 Revision 2 "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide." Typically, healthcare entities implement the NIST SP 800-66 in their work environment.

As a part of the NIST SP 800-66 purpose and scope, it "aims to help educate readers about the security standards included in the HIPAA Security Rule and assist regulated entities in their implementation of the Security Rule." [20] Healthcare entities may also develop a comprehensive network security training program for remote workers, including reinforcement of learning, reminders, ongoing education, webinars, and workshops. Security awareness techniques can be employed through Artificial Intelligence (AI) technologies. However, these steps are essential to help mitigate the potential risk of ransomware attacks caused by work-from-home workers. For example, [21] investigated the use of generative AI to enhance cybersecurity awareness training in the healthcare sector. Their approach incorporates AI-driven simulations and interactive scenarios designed to improve user engagement and retention of critical security concepts. This method has shown promise in strengthening defenses against cyber threats, including ransomware attacks, by making training more relevant and effective. Together, these AI-driven awareness programs empower users to understand ransomware mechanics, recognize high-risk behaviors, and respond effectively.

Moreover, some other National Institute of Standards and Technology (NIST) guidelines and standards, such as the NIST Cybersecurity Framework, NIST Special Publication (SP) 800-171, NIST Special Publication (SP) 800-53 Rev. 5, NIST Special Publication (SP) 800-61 Rev. 2, and NIST SP 1800-11, can be highly efficient for protecting against ransomware attacks.

Lastly, our study's findings establish ongoing research about the relationship between remote work from home in healthcare entities and network security breaches. Future detailed studies are needed to confirm this relationship.

6. Limitations

Certain breaches resulting from ransomware attacks involved multiple breach locations, such as "Electronic Medical Record, Network Server, Other". To ensure the accuracy and consistency of the analysis, these cases were excluded from the study. **Figure 1** and **Figure 2** are excluded from these cases.

7. Conclusion

Ransomware attacks are common in US healthcare data breaches and have many other harmful consequences. However, this study attempts to examine the behavior of ransomware criminals in the US healthcare industry over the past 10 years. The findings show that ransomware attacks occurred most frequently during the COVID-19 pandemic lockdown period (2020, 2021, 2022, and 2023), when work-

from-home was a common business practice for healthcare entities. The findings also show that the network server category has the highest number of breaches during the COVID-19 pandemic. Therefore, this study concluded that healthcare entities need to employ security standards and additional security awareness for work-from-home workers to help protect their entities from potential ransomware attacks.

Acknowledgements

The researchers express gratitude to all peer reviewers for their comments and feedback.

Data Availability Statement

The data supporting the findings of this study are available in the U.S. Department of Health and Human Services-Office for Civil Rights [15]. However, the researchers are not responsible for and have no control over any changes to the availability of data provided by the U.S. Department of Health and Human Services - Office for Civil Rights [15].

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] Muslim, A.K., Mohd Dzulkifli, D.Z., Nadhim, M.H. and Abdellah, R.H. (2019) A Study of Ransomware Attacks: Evolution and Prevention. *Journal of Social Transformation and Regional Development*, **1**, 18-25. https://doi.org/10.30880/jstard.2019.01.01.003

[2] Ryan, M. (2021) Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Springer.

[3] Vanness, R., Chowdhury, M.M. and Rifat, N. (2022) Malware: A Software for Cybercrime. 2022 *IEEE International Conference on Electro Information Technology* (*eIT*), Mankato, 19-21 May 2022, 513-518. https://doi.org/10.1109/eit53891.2022.9813970

[4] Anghel, M. and Racautanu, A. (2019) A Note on Different Types of Ransomware Attacks. Cryptology ePrint Archive.

[5] Chapple, M., Stewart, J.M. and Gibson, D. (2021) (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley and Sons, Inc.

[6] Heuermann, L. (2024) CompTIA Security+ SY0-701 Cert Guide. Pearson.

[7] Wang, K., Pang, J., Chen, D., Zhao, Y., Huang, D., Chen, C., *et al.* (2021) A Large-Scale Empirical Analysis of Ransomware Activities in Bitcoin. *ACM Transactions on the Web*, **16**, 1-29. https://doi.org/10.1145/3494557

[8] Min, N.M., Visoottiviseth, V., Teerakanok, S. and Yamai, N. (2022) OWASP IoT Top 10 Based Attack Dataset for Machine Learning. 2022 24*th International Conference on Advanced Communication Technology* (*ICACT*), PyeongChang Kwangwoon_Do, 13-16 February 2022, 317-322. https://doi.org/10.23919/icact53585.2022.9728969

[9] Atadoga, A., Omaghomi, T.T., Elufioye, O.A., Odilibe, I.P., Daraojimba, A.I. and

Owolabi, O.R. (2024) Internet of Things (IoT) in Healthcare: A Systematic Review of Use Cases and Benefits. *International Journal of Science and Research Archive*, **11**, 1511-1517. https://doi.org/10.30574/ijsra.2024.11.1.0243

[10] Raoof, M.M. (2024) United States Healthcare Data Breaches: Insights for NIST SP 800-66 Revision 2 from a Review of the NIST SP 800-66 Revision 1. *Journal of Information Security*, **15**, 232-244. https://doi.org/10.4236/jis.2024.152014

[11] Spence, N., Niharika Bhardwaj, M. and Paul III, D.P. (2018) Ransomware in Healthcare Facilities: A Harbinger of the Future? *Perspectives in Health Information Management*, **2018**, 1-22.

[12] Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., *et al.* (2022) Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, **3**, e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

[13] Dameff, C., Tully, J., Chan, T.C., Castillo, E.M., Savage, S., Maysent, P., *et al.* (2023) Ransomware Attack Associated with Disruptions at Adjacent Emergency Departments in the Us. *JAMA Network Open*, **6**, e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

[14] Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A. and Varpio, L. (2015) Choosing a Qualitative Research Approach. *Journal of Graduate Medical Education*, **7**, 669-670. https://doi.org/10.4300/jgme-d-15-00414.1

[15] U.S. Department of Health and Human Services-Office for Civil Rights (2024) Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[16] Boadu, G. (2021) Giving Voice to Teachers through Interpretative Phenomenological Research: A Methodological Consideration. *Qualitative Research Journal*, **21**, 408-423. https://doi.org/10.1108/qrj-08-2020-0090

[17] Braun, V. and Clarke, V. (2006) Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, **3**, 77-101. https://doi.org/10.1191/1478088706qp063oa

[18] Al-Habaibeh, A., Watkins, M., Waried, K. and Javareshk, M.B. (2021) Challenges and Opportunities of Remotely Working from Home during Covid-19 Pandemic. *Global Transitions*, **3**, 99-108. https://doi.org/10.1016/j.glt.2021.11.001

[19] McPhail, R., Chan, X.W., May, R. and Wilkinson, A. (2023) Post-Covid Remote Working and Its Impact on People, Productivity, and the Planet: An Exploratory Scoping Review. *The International Journal of Human Resource Management*, **35**, 154-182. https://doi.org/10.1080/09585192.2023.2221385

[20] Marron, J. (2024) Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. National Institute of Standards and Technology.

[21] Zhdanov, D., Caldera, T. and Califf, M.E. (2024) Using Generative AI for Cybersecurity Awareness Training in Healthcare. *Proceedings of the* 19*th Pre-ICIS Workshop on Information Security and Privacy*, Bangkok, 15 December 2024, 1.