What Can the U.S (United States) Learn from the Work of the European Union Agency for Cybersecurity (ENISA) Based on Major Ransomware Attacks in European Hospitals During the Covid-19 Pandemic?

Kendal Eden Taylor

Old Dominion University

IDS 300W

Dr. Kathryn LaFever

November 21st, 2023

Abstract

During 2020, the EU (European Union) suffered a massive amount of cyberattacks against the medical industry. Potential reasons for these attacks include the growing fear of the pandemic, how critical hospitals became, and the value of medical data. Hospitals were unprepared technologically for these attacks, with several of them having major vulnerabilities in their infrastructure. The EU's response to this consists of several new strategies, acts, laws and regulations that the U.S. (United States) can learn from. Some of these involve improving incident response, collaboration, vulnerability and patch management, ransomware laws, and user training. The U.S. can apply aspects of the EU's framework to their own to better defend against ransomware, which is still a relevant threat in cybersecurity. Common ground is found through combining disciplinary insights to determine hospital's weakness, then by how the EU's approach to cybersecurity changed, and finally by understanding what caused the ransomware attacks. There are conflicts between disciplinary findings when it comes to determining why hospitals were so weak in cybersecurity, and why they were targeted so heavily. These conflicts are bridged by taking an interdisciplinary approach to cybersecurity, as there are several factors that can contribute to a successful cyber-attack. Multiple independent variables are used to create a more comprehensive understanding of the EU's response, with one of their most significant improvements being in incident response. This research can be expanded upon by implementing criminology to study cybercriminal behavior. By using multiple disciplines to evaluate EU cybersecurity policy, the U.S. can learn and improve to their own policy.

Keywords: Cybercrime, Medical Cybersecurity, Policy, European Policy

What can the U.S. Learn from the Work of the European Union Agency for Cybersecurity (ENISA) Based on Major Ransomware Attacks in European hospitals During the Covid-19 Pandemic?

This research paper explores the issue of what the U.S. (United States) can learn from the work of the EU (European Union) based on the major ransomware attacks that occurred against European hospitals during Covid-19. What can the U.S. learn from the work of the European Union Agency for Cybersecurity (ENISA) based on major ransomware attacks in European hospitals during the Covid-19 pandemic? To answer this question, this paper utilizes three different fields of study. They are Cybercrime, Medical Cybersecurity, and Policy Studies. Cybercrime explains the surge of attacks that occurred during the pandemic, and why ransomware was used so heavily against the medical industry. Medical Cybersecurity addresses how hospitals are vulnerable to ransomware, the factors that contribute to this, and how their security posture can improve. Policy studies evaluate the way that the EU responded to the attacks, and what the U.S. can learn from them. An interdisciplinary approach to my research accomplishes a thorough analysis of why the healthcare industry was targeted so heavily and what we can learn from the ENISA's response. This research relates to my major as it is Cybersecurity. Several of my courses have already discussed ransomware, as it is still a relevant threat in the field. This research paper can help to gain insight into why the pandemic attacks occurred, how the EU responded, and what the U.S. can learn from it.

Definitions

Computer viruses, vulnerabilities, phishing, GDPR (General Data Protection Regulation) and ransomware are among the key terms that are utilized in this article. *Ransomware* is defined by the FBI (Federal Bureau of Investigation) as "a type of malware that encrypts computer files

and prevents access to them until a ransom is paid." (FBI, 2022). According to Thusar P. Parikh, a cybersecurity professor and research scholar from the University of Patan, a *vulnerability* is "A weakness in a system or its design that allows an intruder to execute commands, access unauthorized data, and/or conduct denial-of service attacks." (Parikh, T. 2017). As defined by Elmer EH Lastdrager, a cybersecurity professional at the University of Twente, *phishing* is "an act of deception whereby impersonation and or manipulation is used to obtain information from a target." (Lastdrager, E. 2014). Peter Szor, a computer virus and security research expert from the University of Pannonia, defines *computer viruses* as "A program that recursively and explicitly copies a possibly evolved version of itself." (Szor, 2005). Sean Sirur, a cybersecurity professor at the University of Oxford, defines the *GDPR* as, "An act that aims to reform how organizations view and control the personal data of private EU citizens." (Sirur, 2018).

Cybercrime

In April 2020, the International Criminal Police Organization (INTERPOL) published a report cautioning the world, warning of an increase in cyberattacks (Muthupalaniappan, M., & Stevenson, K, 2020). According to data from the Federal Bureau of Investigation (FBI), cybercrime increased by 400% during the pandemic (FBI, 2020). Cybercriminals found the growing fear and uncertainty caused by the pandemic opportune, as well as the world's increasing reliance on technology.

A potential reason for this increase in cybercrime could be the value of medical data. Medical data is far more valuable than credit card fraud or other online scams. This is because medical information encompasses everything from a patient's medical history to their medical prescriptions. Hackers can use this information for profit or to commit future fraud, such as creating fake prescription orders using stolen medical data. (Petersen, 2015). The more

information within a database, the more valuable it is to hackers. This is another reason ransomware was so effective against the medical industry.

One of the ways that these attacks occur is through phishing. An example of this is a successful ransomware against the Benešov Hospital during 2020, where a series of phishing emails were sent across the hospital using a link to a fake invoice (Filipec, O. & Plášil, D. 2021). A hospital worker clicked on the link, initiating the attack. Hours after this, the hospital's IT (Information Technology) team received phone calls regarding slow systems and an inability to reach certain websites. Once the team realized what had occurred, it was already too late, as the entire hospital network and database was encrypted by ransomware.

Medical Cybersecurity

Cybercrime attacks result in limited hospital functioning, often causing hospitals to have to go back to pen-and-paper charting to administer care. This type of interruption was unacceptable and potentially life-threatening, as hospitals could not afford to be shut down for a second during the pandemic. This fact was heavily exploited by hackers, as hospitals were more likely to give in to the ransom to resume functionality. Paying a ransom is strongly discouraged, as it just shows attackers that their attack model works. However, hospitals that do not pay ransoms can spend months rebuilding their systems (McGlave, C. et. Al, 2023). "No hospitals, healthcare facilities or even medical research laboratories, specifically those trying to develop COVID-19 tests and vaccines, were spared during this surge in ransomware attacks." (Gallagher & Bloomberg, 2020).

Hospitals and other medical institutions often put cybersecurity 'on the backburner' of their list of priorities. They are often forced to make budget cuts in this sector to fund staff and front-line services (Minaar, 2022). Consequently, the Covid-19 surge of cyber-attacks exposed

how unprepared hospitals were to deter and recover from cyber-attacks. Hospital employee negligence was a primary cause of ransomware, along with a lack of user awareness training. Heavily outdated systems were also frequently found within hospitals that had suffered ransomware attacks (Hoffman, 2020). Another issue is that of a lack of network segmentation. This vulnerability means that every device in the hospital's infrastructure, such as the computers, MRIs, CAT Scanners, and X-RAY machines for example, were all using the same network. Consequently, when an attacker compromises a singular computer in the infrastructure, the entire network is infected, including life-saving devices (Tervoort et. Al, 2020).

As mentioned, many hospitals and healthcare services failed to implement even basic security measures. In response to this threat, many hospitals had to respond by implementing drastic security changes to their vulnerable systems (Minaar, 2022). These changes include establishing vulnerability management routines, rigorous updates to their systems, creating an incident response team, and establishing frequent employee cybersecurity training to name a few. Another change is creating offline and offsite backups of data that are regularly tested and updated. This way, when a ransomware attack occurs, hospitals can still have some form of access to their data until their systems are recovered (Pino, 2022).

Policy Studies

The European Union has taken several measures to tackle cybersecurity threats. In December 2020, the EU Cybersecurity Strategy was presented. It aims to strengthen the EU's resilience against various cyber threats by focusing on three principles. They include the ability to prevent and respond to cyberattacks, improving operational capacity to better respond to cyber incidents, and establishing cooperation globally between organizations during an attack. This strategy was then adopted and concluded in March 2021 (European Council of the European

Union, 2023). In addition to this, during September 2022, The ENISA proposed the Cyber Resilience Act. This framework contains several strategies to help improve responsiveness to cyber-attacks, including the launch of a “Cyber Rapid Response Team.” and a multinational “Cyber and Information Domain Coordination Centre” that encourages communication between member states (Tasheva, I. & Kunkel, I. 2022).

During the surge of cyberattacks, ENISA released an article providing information to healthcare organizations for when an attack occurs. They include sharing the information with healthcare staff, freezing any activity within a compromised system, and swiftly notifying the IT team and incident response team (ENISA, 2020). ENISA has also established standards to mitigate ransomware threats in hospitals. According to ENISA's threat landscape in 2021, they are: “substantial investments in backup strategies, implementing segregation of duties, network segmentation, and reviewing management response and recovery plans periodically.” (Antonio M. Villamor, Jr, 2023).

In 2022, it was reported that the global ransomware payments amount to almost $457 million USD (Chainalysis Team, 2023). The European Union has set up laws and regulations to provide consequences for those who pay the ransom, such as violating the GDPR (General Data Protection Regulation). Organizations who pay the ransom can risk violating GDPR compliance, which can result in fines and reputational damage. Despite this, many Europeans have given into the ransom. One of the requirements through the GDPR is for reporting ransomware. This establishes that organizations must notify the local data protection authority within 72 hours of breach detection (Antonio M. Villamor, Jr, 2023).

Common Ground

This interdisciplinary research has disclosed three major common ground findings. First, the increase in cybercrime against hospitals could have been caused by the growing fear around the pandemic, the profit of medical data theft, and how critical hospital services became during the pandemic. This utilizes the disciplines medical cybersecurity and cybercrime. Second, cybersecurity was a weakness in hospitals. There were several major vulnerabilities that were heavily exploited by hackers during the pandemic. This also utilizes cybercrime and medical cybersecurity. Finally, the EU has proposed several policies to effectively combat ransomware by improving cybersecurity policy and standards within organizations. This finding utilizes cybercrime and policy studies. Without interdisciplinary research, the explanation for why hospitals were targeted so heavily and effectively would not have been properly addressed. The EU also would not have been able to establish specific policies and standards that understand the multiple issues within medical cybersecurity.

Disciplinary Conflicts

One of the conflicts between the disciplinary findings comes from determining the weakness in hospital infrastructure, and why they were targeted so heavily. Policy studies address that a lack of cybersecurity acts and guidelines were responsible, while medical cybersecurity urges that hospitals failing to implement basic security measures were. Cybercrime advocates that the value of medical data and the urgency of the pandemic were responsible. A way to bridge the differences between these insights is by understanding that there is no individual explanation for why cyberattacks occur. A multidisciplinary approach to cybersecurity is much more beneficial as it encompasses several factors as to why cyberattacks occur. Each attack depends on which attack strategy hackers use, what type of data they are after and different weaknesses that led to the successful attack.

Constructing a More Comprehensive Understanding

Utilizing multiple independent variables, a more comprehensive understanding can emerge from this research. One of the biggest changes the EU implemented in response to the ransomware attacks was an improved approach to incident response. From the EU's work on this, the U.S. can learn that collaboration and communication during major cyber incidents is essential. The EU has also established multiple new frameworks regarding patch management, vulnerability assessment, security audits, significantly improved user training, and much more. Utilizing this, the U.S. can work to reestablish their current cybersecurity framework based on the changes the EU has made. This can help the U.S. better prepare for ransomware attacks and cyber incidents.

Reflecting, Testing and Communicating

To build upon this issue in future research, criminology could be an additional discipline used to investigate cybercriminal activity. There are several links between criminology, cybersecurity, and cybercrime. Studying the minds of cybercriminals can help to further understand why they chose to potentially endanger lives by targeting hospitals. It can also help to utilize criminology in EU and U.S. cybersecurity policy to better prepare and deter cybercriminals. Research in this field can help to further understand behavior patterns, motivations, and psychological traits of cybercriminals. Understanding this can also help to identify potential warning signs of a cybercriminal breach, which can be integrated into cybersecurity policy (Dupont, B. & Whelan, C. 2021).

Conclusion

In conclusion, this article addresses what the U.S. can learn from the EU's response to the Covid-19 ransomware attacks. This is accomplished by understanding why the surge of attacks occurred, the factors that contributed to hospital vulnerability, and an evaluation of how the EU responded. The U.S. can take the work and the mistakes of the EU into account when creating their own policies. Common ground is found by attempting to determine the cause of the attacks, and weaknesses in hospitals. Conflicts in this study occur between disciplines, as each has their own insight into why

hospitals were attacked so heavily. A more comprehensive understanding comes from utilizing multiple independent variables when analyzing the EU's response. This topic can be expanded upon by employing fields such as criminology. This research can help to address the threat of ransomware and learn how the U.S. can best respond.

References

Antonio M. Villamor, Jr. (2023, April 19). ENISA's Threat Landscape and the Effect of Ransomware. *ISACA. 2*(1). *https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/enisas-threat-landscape-and-the-effect-of-ransomware*

Chainalysis Team. (2023, January 19). Ransomware Revenue Down as More Victims Refuse to Pay. *Chainalysis*. *https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/*

Dupont, B., & Whelan, C. (2021, March 27). Enhancing Relationships Between Criminology and Cybersecurity. *Journal of Criminology*, *54*(1), pg. 76-92. https://doi.org/10.1177/0004865821100392

ENISA. (2020, May 11). Cybersecurity in the Healthcare Sector During COVID-19 Pandemic. *ENISA*.

https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

European Council of the European Union, (2023, July 19) Cybersecurity: How the EU Tackles Cyber Threats. *Consilium.* *https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/*

FBI. (2022). Ransomware. *Federal Bureau of Investigation.* https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Filipec, O & Pláŝil, D. (2021, June 20). The Case of the Benešov Hospital Hit by Ryuk Ransomware, and Lessons Learned. *Obrana a Strategie. 21(1),* pg. 27-52. *10.3849/1802-7199.21.2021.01.027-052*

Gallagher, R. & Bloomberg. (2020, April 1). Hackers 'Without Conscience' Demand Ransom From Dozens of Hospitals and Labs Working on Coronavirus. *Fortune Magazine.* *https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/*

Hoffman, S. A. E. (2020, July 9). Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure. *World Libraries. 24*(1). *https://worldlibraries.dom.edu/index.php/worldlib/article/view/588*

Lastdrager, E, E. (2014, September 3). Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature. *Crime Sci. 3*(9). https://doi.org/10.1186/s40163-014-0009-y

McGlave, C. C. Neprash, H. & Nikpay, S. (2023, October 4). Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients. *Social Science Research Network.* *https://doi.org/10.2139/ssrn.4579292*

Minaar, Anthony. (2022, October 13). Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic. *Acta Criminologica. 34*(3), pg. 154-185. *10.10520/ejc-crim_v34_n3_a10*

Muthuppalaniappan, M. & Stevenson, K. (2020, September 27). Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Heal*th *Care*. 33*(1)*. *https://doi.org/10.1093/intqhc/mzaa117*

Peter Szor, P. (2005). *Art of Computer Virus Research and Defense*. Pearson Education.

Petersen, A. (2015, March 17) Cyberattack at Health Insurer Exposed Data on 11 Million Customers – Including Medical Information. *The Washington Post.* *https://www.washingtonpost.com/blogs/the-switch/wp/2015/03/17/cyberattack-at-healthinsurer-exposed-data-on-11-million-customers-including-medical-information/*

Pino, L. (2022, February 28). Improving the Cybersecurity Posture of Healthcare in 2022. *HHS.gov.* *https://www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html*

Sirur, S. Jason, R.C. & Webb, H. (2018, January 15). Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR), *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*. 8(*7),* pg. 88-95. https://doi.org/10.1145/3267357.3267368

Tasheva, I. & Kunkel, I. (2022, November 20). In a Hyperconnected World, is the EU Cybersecurity Framework Connected? *European View. 21*(2*)*, pg. 186-195. *https://doi.org/10.1177/17816858221136106*

Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. & Marquering, H. (2020, March 30). Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access*, 8(4), *10.1109/ACCESS.2020.2984376.*

Tushar, P., & Parikh. (2017, June 6). Cyber security: Study on Attack, Threat, Vulnerability. *International Journal of Research in Modern Engineering and Emerging Technology, 5*(6).

https://www.raijmr.com/ijrmeet/wp-content/uploads/2017/12/IJRMEET_2017_vol05_issue_06_01.pdf