RISK TRENDS BY INDUSTRY: AN EMPIRICAL STUDY IN RANSOMWARE TARGET TRENDS

by

Tom Williams III

B.S., Georgia Southern University, 2017

M.S.I.T., Middle Georgia State University, 2019

A Research Paper Submitted to the School of Computing Faculty in Partial

Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

Risk trends by industry: an empirical study in ransomware target trends

Tom Williams III, *Middle Georgia State University, tom.williams@mga.edu*

Abstract

Cybersecurity risk and the use of ransomware attacks have cost organizations millions of dollars globally over the last decade. These costs are rising as ransomware payment demands increase and malicious tooling becomes more sophisticated. The impact of these attacks is difficult to measure due in large part to fragmented data and no centralized oversight. Additional challenges stem from the technological evolution of ransomware attack variants along with ease of access to tooling provided by ransomware gangs. In this study, cybersecurity and ransomware risk are observed across industries to better understand the risk to industries targeted by ransomware operators. This study also explores several challenges related to risk mitigation for ransomware attacks. The global impact is significant, and ransomware continues to hit headlines as organizations impacted release information on security incidents.

Keywords: ransomware, trends, risk, cybersecurity, cyber-criminals, industry

Introduction

Ransomware attacks have increased significantly over the last several years and had a major financial impact on businesses and organizations around the world (Koomson, 2021). These attacks were on the rise before the COVID-19 Pandemic and the shift to work-from-home was in large part taken advantage of by cybercriminals (ABA, 2022). Threat actors and ransomware operators are targeting healthcare providers, critical infrastructure, utility services, and municipalities (CISAa, 2022).

The increase in profitability combined with ease of access to ransomware tooling has contributed to the spread of ransomware attacks worldwide (CISAa, 2022). In addition, ransomware malware payloads are evolving constantly, and attack volumes are expected to continue increasing (Robin, 2021). While there is a risk for anyone to become a target, ransomware is primarily distributed through phishing campaigns to organizations and businesses. These targets have valuable data and financial success has driven more cybercriminals to leverage ransomware as an attack (CISAa, 2016).

It is critical ransomware attack trends are objectively studied across industries to answer questions related to those targeted. In 2020, ransomware attackers generated over $300 million in revenue (Chainalysis, 2021). Ransomware is considered one of if not the biggest threats to organizations in 2022 with a projected cost reaching $265 billion by 2031 (Rubin, 2021). This is a significant increase from the $27 million CryptoLocker generated from 2013 – 2015. Assessing the impact from an industry perspective has the potential to provide awareness to those that need stronger countermeasures to protect their infrastructure. The purpose of this study is to observe how the evolution of ransomware and ransomware services have influenced risk across industries. This research will answer the following question:

RQ: How have ransomware target trends changed across industries in the last five years as RaaS services became operational?

Literature Review

Ransomware has been making headlines for over a decade and continues to be a challenging issue for cybersecurity experts, individuals, and organizations around the world. Within the United States, individual data, critical infrastructure, financial systems, and medical information have been compromised at alarming rates (Nad, 2022). Rapid evolution in technology, lack of data sharing, and constant shifts in online behavior pose a major challenge to law enforcement when attempting to combat cybercrime utilizing ransomware (Lee, 2022). Additionally, collaboration among private industry, researchers, and law enforcement is often structured by personal relationships rather than trust between all parties (Lee, 2022). This is further complicated due to challenges related to jurisdiction given that ransomware payloads cross borders within cyberspace. It can be inferred that experts are fighting an uphill battle because ransomware strains are evolving fast and becoming more difficult to counter. Not only are the technologies evolving and becoming more sophisticated –ransomware operators are also joining together to form "ransomware gangs". These organized groups have notably increased the volume of attacks through organized ransomware operations (Nad, 2022).

As the name implies, ransomware operators often demand payment to restore access to the data affected. Data is modified through the use of two primary types of ransomware: those that are considered lockers and those that employ cryptography to encrypt data rendering it virtually impossible to access (Richardson & North, 2017). This often leaves the systems that rely on the data inoperable and brings the organization's processes and operations to a halt (CISA, 2023).

Despite the recent resurfacing of ransomware attacks, ransomware dates to 1989 when Joseph Popp, a biologist, created the first-ever ransomware attack. The payload for this attack was deployed using floppy disks by the post office and targeted the World Health Organization (The strange history, 2017). The attack, often referred to as the AIDS Trojan, relied on a set number of reboots before locking the machine. Once the machine was locked, the malware demanded payment of $189 USD be sent to an address in Panama (The strange history, 2017). Throughout the following twenty-plus years, ransomware was less of a threat and all but disappeared (Nad, 2022).

The modern wave of ransomware variants began between 2013 and 2016 with the release of CryptoLocker (Richardson & North, 2017). CryptoLocker was one of the first to use anonymous payment systems and the creators generated over $27 million in revenue by 2015 (Richardson & North, 2017). Other ransomware variants such as Samas and Locky were later observed in cyberspace primarily targeting businesses and individuals in 2016. Distribution techniques such as phishing, social media services, and drive-by downloads are primarily used to infect victims' systems (CISA, 2016). Threat actors also leverage search engine ads as an alternative phishing technique to distribute their ransomware payload. These techniques often impersonate legitimate software and services to trick users into clicking their ad links when using search engines. The goal is to distribute ransomware or steal credentials for crypto exchanges and financial institutions. The link provided in the ad takes users to a webpage disguised as the legitimate site for the software application. Links to download the software simply direct users to malicious applications (IC3, 2022). IC3 released a Public Service Announcement in December 2022 warning the public of these attacks and how to identify them.

Today, ransomware attacks and distribution techniques have advanced well beyond the AIDS Trojan and CryptoLocker; however, still aim to primarily extort money from the victim in exchange for restored access to the encrypted or locked files. Further pressure is put on the victim through diversified approaches to extortion which can include threats to release stolen data, notify shareholders or other parties, and disruption to network operations or Internet access (CISAa, 2022). In many cases, the attackers exfiltrate data as proof of access, then use the data in threats to release, or evidence to show "proof of life" so to speak for those considering paying the ransom.

The Ransomware operator's financial medium of exchange is typically a form of cryptocurrency, which is also known as virtual currency (Alfieri, 2022). To understand why threat actors that distribute ransomware rely primarily on cryptocurrency it is worth exploring how cryptocurrency was designed and functions. Cryptocurrency is decentralized – completely unregulated with no central control or administration. The system behind cryptocurrency is made up of peer-to-peer exchanges that log information in what is known as a blockchain. The blockchain is essentially the historical ledger of transactions that is publicly accessible; however, the users of the blockchain are not easily identifiable due to the use of wallet addresses. These wallet addresses don't necessarily reference a person by name but rather a key value used to sign transactions. Only if the owner is identified can the virtual currency transactions be traced and tied to the user (Alfieri, 2022).

The complete financial impact of ransomware has been challenging to measure given the targeted organizations and individuals are globally distributed and relevant data fragmented; however, through information released publicly by organizations, there is a glimpse of the demands being made by ransomware threat actors. In 2021, CNA Financial, one of the largest insurance companies in the United States paid $40 million to regain access to their systems following a ransomware attack (Mehrotra & Turton, 2021). Victims often attempt to remediate through the recovery of data through backups, cyber insurance, professional restoration services, paying the ransom, or through negotiations with the threat actor directly (Nad, 2022). In the case of CNA Financial, they accepted the risk of paying the ransom. This is one of the largest ransomware payouts ever recorded. In some situations, the ransom demand increases over time as an attempt to apply pressure on the victim for more immediate payment.

In recent years, the FBI has published warnings that ransomware operators are getting even more intelligent when it comes to targeting organizations (FBI, 2022). Factors that impact a business's decision to pay the ransom are also getting more complex. Leaning into the extortion technique, ransomware operators are now collecting data on potential targets related to corporate mergers and acquisitions to further pressure the victim into paying the ransom (Gatlan, 2021). There may be legal or good faith obligations to protect sensitive data either for government requirements or shareholders. Release of such data may have high financial consequences in the form of fines or company value. In some cases, threat actors are gathering and assess data within the corporate network once they've gained access rather than relying on publicly accessible information. An example of this in cyberspace is how REvil, a ransomware "gang", announced that they have considerations to adding auto-email logic to their payload that would alert stock exchanges in an attempt to manipulate the stock value (Gatlan, 2021). The goal is to put as much pressure as possible on the victim for payment.

In 2021, ransomware operatives began offering professional services and support for ransomware distribution. The Ransomware as a Service (RaaS) solutions take it a step further to enable threat actors ease of access to leverage ransomware as an attack methodology for their targets (CISAa, 2022). Additionally, some RaaS operations include 24/7 support centers and functions with a structured business model (CISA, 2022a). These more professional operations provide malicious services in exchange for monetary gain thereby facilitating increases in ransomware distribution by those that may not otherwise have the technical means to carry out their attack.

Since surfacing, RaaS offerings quickly left a mark on various industries which include the Colonial Pipeline Company incident in May 2021. The United States Department of State issued an alert in November 2021 urging anyone with information on the DarkSide ransomware variant to contact the FBI (FBI, 2022). This alert was incentivized with up to a $10 million reward for information that leads to the identification or location of individuals involved (U.S. Department of State, 2021).

Within the United States, ransomware is considered a threat to national security (CISA, 2023). The same can be said for the use of cryptocurrency as cyber and terrorist groups adopt its use (Alfieri, 2022). The

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was passed to address the lack of comprehensive data on ransomware and the use of cryptocurrency or virtual currency payments (CIRCIA). Additionally, CIRCIA authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to take action if an entity fails to provide required reporting (CISA, 2022b). This is an attempt to solve one of the biggest challenges to getting ahead of ransomware threats: data sharing and collaboration among those attempting to counter the global threat. Reporting is lacking in some cases due to victims assuming law enforcement cannot assist (Nad, 2022). The collection of this data along with the collaboration among law enforcement, industry, and cyber security researchers is integral to countering ransomware globally.

Methodology

Data collection involved leveraging the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. This database is freely accessible to the public and contains corporate information on both operations and financials (SEC, 2018). Additionally, these reports provide information on business conditions in various sections of each form type. Navigating the database either by manual search or API gives options for accessing and collecting data. The authenticity and reliability of this data is ensured given companies are required to provide annual and factual reports for specific events by the federal government (SEC, 2018). Using the API several report types can be extracted. Form 10-K for annual filings, Form 10-Q for quarterly, and Form 8-K for current report filings. For this research, the data of interest exists within the Risk Factor information which is reported within Item 1A of Form 10-K submissions (SEC, 2018).

The starting point for building the dataset involved downloading a bulk archive ZIP file which is recompiled nightly and provided on the SEC's website. This archive contains filing history for companies broken out as JSON files where the filename contains the Central Index Key (CIK) of each company. The CIK is used as a primary key within the dataset. A Python script was written that captured the CIK within the filename and searched the text of each submission's JSON file for Form 10-K filings within the last five years. For companies with filings on record, the company names and CIKs were extracted and inserted into an SQLite database table. The total number of companies with recent Form 10-K filings on the initial pass was 37,696.

It is necessary to ensure that the dataset is complete and contains filings within the last 5 years for each company. Validation checks were required for each datapoint extracted. A Python script was written to validate the result returned from the API and extract the datapoints of interest using the company CIK as a key reference. The Committee on Uniform Securities Identification Procedures (CUSIP) information was used to identify the industry, sector, ticker, and stock exchange of the company. This includes being able to programmatically extract via the SEC's API the CIK, company name, industry, sector, CUSIP, stock ticker, and stock exchange of each company. An additional validation was put in place to ensure each company had a Form 10-K filing on record for each of the last five years. In addition, the filing URLs for each Form 10-K filing were extracted and inserted into the database. If CUSIP or Industry was blank, those companies were ignored and excluded from the collection process. Companies with complete information were inserted into the SQLite database.

Lastly, using the information captured and stored in the database, a Python script was written to download the Form 10-K filings via the captured URLs from the collection process. These filings were stored as TXT files for later use in the text analysis phase.

After the validation of company information, the dataset contained 2,928 companies with a total of 14,640 Form 10-K filings spanning the last 5 years.

For each company and year, the text within the Item 1A Risk Factors was extracted as a corpus to be analyzed using Natural Language Parsing (NLP) text analysis methods written in Python. The analysis process searched for the top 5 ransomware variants by name along with “cybersecurity”, “cyberattack” and common word associations for ransomware, including the term “ransomware”. Ransomware variants included in the analysis include REvil, Maze, Ryuk, WannaCry, and NetWalker (CrowdStrike, 2022).

A separate database table was created to capture Boolean values as indicators as to whether these terms were found in the risk corpus for each report during the text analysis phase. Given that the data being analyzed has very explicit text referencing, text wrangling was not considered to yield different results for the text analysis phase. The analysis process did not include conversion to lowercase, removal of punctuation and stop words, or stemming for the text corpus of each report. The text analysis explicitly analyzed the report data for the word associations described.

The data was analyzed through several SQL statements that aggregated the reports of risk per year by company and industry. The results were then imported into Microsoft Excel which was used as the tooling to build the visual figures.

Results

Analysis of the data focused on the overall reported risk and top 20 industries from the dataset reporting risk in the year 2022 (E.g. Percentage of companies in the Semiconductor industry that reported risk in 2022 was 1.47%). The total number of companies in the dataset is 2928 with representation from 146 industries.

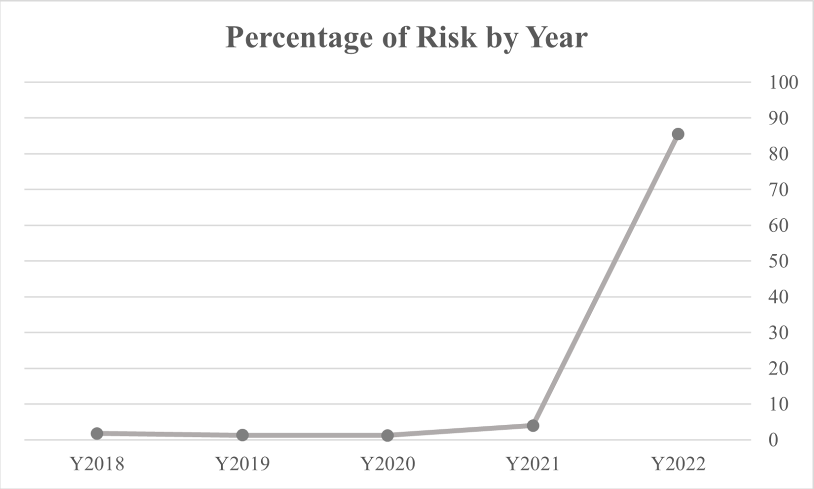

Figure 1: Percentage of companies reporting risk by year for the last 5 years.

The data revealed a substantial increase in reported risk across companies and industries between 2020 and 2022. By 2022, over 85% of companies are reporting risk.

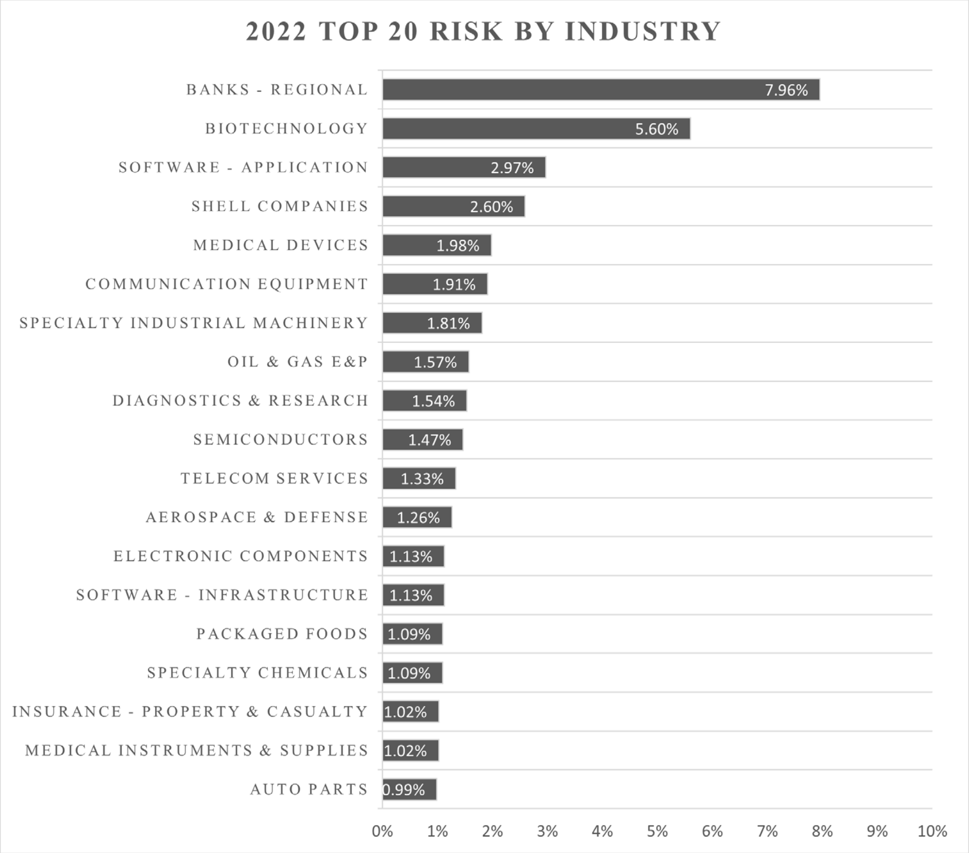

Figure 2: Top 20 Industries Reporting Ransomware and Cyber Security Risk in 2022
Note. Figure 2 shows the Top 20 Industries by Reported Risk for the year 2022 in order by the highest first. Number of Industries = 146, total companies N = 2928.

Table 1: *Percent of companies by industry reporting risk by year for the last 5 years.*

Industry	2022	2021	2020	2019	2018
Banks - Regional	7.96%	0.07%	0.03%	0.07%	0.10%
Biotechnology	5.60%	0.20%	0.03%	0.14%	0.20%
Software - Application	2.97%	0.17%	0.17%	0.10%	0.17%
Shell Companies	2.60%	1.50%	0.00%	0.00%	0.00%
Medical Devices	1.98%	0.07%	0.03%	0.00%	0.03%
Communication Equipment	1.91%	0.00%	0.03%	0.00%	0.00%
Specialty Industrial Machinery	1.81%	0.03%	0.00%	0.00%	0.07%
Oil & Gas E&P	1.57%	0.03%	0.00%	0.03%	0.03%
Diagnostics & Research	1.54%	0.10%	0.03%	0.07%	0.03%
Semiconductors	1.47%	0.07%	0.03%	0.03%	0.00%
Telecom Services	1.33%	0.07%	0.07%	0.00%	0.00%
Aerospace & Defense	1.26%	0.03%	0.00%	0.07%	0.00%
Electronic Components	1.13%	0.00%	0.00%	0.00%	0.00%
Software - Infrastructure	1.13%	0.00%	0.03%	0.03%	0.07%
Packaged Foods	1.09%	0.00%	0.00%	0.03%	0.03%
Specialty Chemicals	1.09%	0.00%	0.03%	0.03%	0.10%
Insurance - Property & Casualty	1.02%	0.03%	0.00%	0.00%	0.00%
Medical Instruments & Supplies	1.02%	0.03%	0.00%	0.00%	0.03%
Auto Parts	0.99%	0.10%	0.00%	0.00%	0.03%

Note. Number of Industries = 146, total companies N = 2928.

Conclusion

The purpose of this study was to gain a better understanding of ransomware risk from an industry perspective following the introduction of RaaS. Based on the reported risk and timeline in 2021 of RaaS services becoming widely available it can be inferred that RaaS services may have contributed to the steep increase in ransomware and cybersecurity risk being reported. The reported risk was less than 10% between the years 2018 and 2021. By 2022, over 85% of companies were reporting risk as observed in Figure 1.

In Figure 2, 7.96% of the companies reporting risk are in the *Banks – Regional* industry which is up from 0.10% in 2018. Interestingly, *Biotechnology* companies are in second at 5.60% of the total sample reporting risk. The findings suggest RaaS has had a major influence on cybersecurity risk.

Ransomware operators seek financial gain from their targets which may explain the motive for those industries that are reporting the highest percentage of risk. Coincidentally, *Biotechnology* entities came more into focus during the COVID-19 pandemic. Between 2018 and 2020, *Biotechnology* companies were trending downward in risk; however, in 2021 there was a sharp increase that exceeded previous years. The sense of urgency for a solution to counter the Coronavirus may have made these entities higher value targets as their research data would be integral to their efforts. Loss of data access or threats of exfiltration would create an immense amount of pressure for paying the ransom.

Additional event correlation suggests that ransomware targets shift based on the criticality of operations, or potentially the lucrative nature of services provided by the industry. An example of this is how *Health*

Information Services ranked 31 in 2019 and rose to rank 8 in 2021 during the heart of the COVID-19 pandemic. By 2022, the *Health Information Services* industry ranked 75th.

Interestingly, the findings reveal that executive leadership is becoming increasingly aware of the risks associated with ransomware and cybersecurity. The filing data analyzed is submitted to the SEC by executive leadership and it can be inferred that their level of awareness is increasing.

Conclusion

In summary, these research findings contribute to the body of evidence suggesting RaaS services have closely influenced the widespread, global increase of risk across industries. The growing prevalence of ransomware as an attack is proving highly lucrative for threat actors and challenging to counter for industry professionals. Furthermore, ransomware payment demands are hitting record highs as malicious tooling becomes more sophisticated and even more difficult to mitigate.

The present research contributes sufficient evidence suggesting that RaaS services are increasing cybersecurity risk to organizations. This study also suggests ransomware target trends are influenced by external factors that determine the criticality of business services or operational risk. Recall that ransomware operators are seeking more creative ways to pressure victims. Disruption of operations for services deemed critical has implied pressure for a prompter ransomware payment. This study suggests environmental events that capture national or global focus have the potential to shift those targeted. Regardless of focused targets, since the availability of RaaS, there is evidence of increased volumes of attacks as revealed in the study findings across most industries.

There are limitations to this study which include the lack of accessible, centralized information on ransomware attacks. Additionally, the sentiment or severity of the risk reported in the filings is undetermined. This study can only assume risk exists given that ransomware and cybersecurity were reported within the Form 10-K Risk Factors section. The assumed sentiment is that these entities have valid reasons to believe there is a concern. This study is also unable to determine if there were incidents or attempted cyber-attacks that prompted the reason for reporting risk. Lastly, more data is required to determine the signaling mechanisms that raised concerns.

For future research, it would be beneficial to expand the number of companies for a larger sample size. There is much work to be done to determine more accurate reasoning behind the reported risk along with the signaling mechanisms leveraged. Analysis of ransomware variants, financial impact, and the number of attacks per variant would also be valuable for future research.

References

ABA. (2022, March 16). *The Ransomware Epidemic: Criminals Taking Advantage of Those Working from Home—Including Lawyers and Media Companies*. American Bar Association. Retrieved January 3, 2023, from https://www.americanbar.org/groups/communications_law/publications/communications_lawyer/2022-winter/the-ransomware-epidemic-criminals-taking-advantage-those-working-homeincluding-lawyers-and-media-companies/

Alfieri, C. (2022). Cryptocurrency and National Security. *International Journal on Criminology*, *9*(1), 21–48. https://doi.org/10.18278/ijc.9.1.3

Chainalysis. (2022, May 20). *Ransomware skyrocketed in 2020, but there may be fewer culprits than you think*. Chainalysis. Retrieved October 9, 2022, from https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021/

CISA. (2016, March 31). *Ransomware and Recent Variants*. CISA. Retrieved January 12, 2023, from https://www.cisa.gov/uscert/ncas/alerts/TA16-091A

CISA. (2022a, February 9). *2021 Trends Show Increased Globalized Threat of Ransomware*. Cybersecurity & Infrastructure Security Agency. Retrieved October 9, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

CISA. (2022b). *Cyber incident reporting for critical infrastructure act of 2022 (CIRCIA)*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved January 21, 2023, from https://www.cisa.gov/circia

CISA. (2023, January 21). *Stop Ransomware Resources*. CISA | Stop Ransomware. Retrieved January 21, 2023, from https://www.cisa.gov/stopransomware/resources

CrowdStrike. (2022, October 13). *Most common types of ransomware: CrowdStrike*. CrowdStrike. Retrieved October 23, 2022, from https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/

FBI. (2022, August 22). *FBI Philadelphia urges Cybersecurity Awareness*. FBI. Retrieved January 10, 2023, from https://www.fbi.gov/contact-us/field-offices/philadelphia/news/press-releases/fbi-philadelphia-urges-cybersecurity-awareness

Gatlan, S. (2021, November 2). *FBI: Ransomware targets companies during mergers and acquisitions*. BleepingComputer. Retrieved January 6, 2023, from https://www.bleepingcomputer.com/news/security/fbi-ransomware-targets-companies-during-mergers-and-acquisitions/

IC3. (2022, December 21). *Internet crime complaint center (IC3): Cyber criminals impersonating brands using search engine advertisement services to defraud users*. Internet Crime Complaint Center (IC3) | Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users. Retrieved January 10, 2023, from https://www.ic3.gov/Media/Y2022/PSA221221

Koomson, J. (2021, October 19). *Rise of ransomware attacks on the education sector during the COVID-19 pandemic*. ISACA. Retrieved October 9, 2022, from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic

Lee, J. (2022). Prospects, Barriers, and Future Directions of Cybercrime Research and Investigations. *Translational Criminology*, *22*, 9–11.

Mehrotra, K., & Turton, W. (2021, May 20). *CNA financial paid hackers $40 million in ransom after March cyberattack*. Bloomberg.com. Retrieved January 21, 2023, from https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

Nad, K. (2022). Ransomware Warfare: Exploring Global and Private Negotiations to Help U.S. Victims Respond to the Threat. *Cardozo Journal of Conflict Resolution*, *23*(1), 257–299.

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13*(1), 10–21.

Rubin, A. (2021, December 7). *Ransomware is the greatest business threat in 2022*. Ransomware Is the Greatest Business Threat in 2022. Retrieved October 9, 2022, from https://www.nasdaq.com/articles/ransomware-is-the-greatest-business-threat-in-2022

SEC. (2018, September 5). *Using EDGAR to Research Investments*. SEC Emblem. Retrieved October 9, 2022, from https://www.sec.gov/oiea/Article/edgarguide.html

The strange history of ransomware [Radio broadcast transcript]. (2017, May 16). PRI's The World. https://link.gale.com/apps/doc/A495871367/LitRC?u=maco12153&sid=ebsco&xid=205016e8

U.S. Department of State. (2021, November 4). *Darkside ransomware as a service (RAAS) - united states department of state*. U.S. Department of State. Retrieved January 22, 2023, from https://www.state.gov/darkside-ransomware-as-a-service-raas/