ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 11, November 2024

Ransomware Rising - Understanding, Preventing and Surviving Cyber Extortion

[1] David Michael Berry

[1] Identity Ward, Canada
Corresponding Author Email: [1] david.michael.berry@identityward.com

Abstract— Ransomware attacks have surged in recent years, posing severe threats to organizations across various sectors. This paper provides a comprehensive analysis of ransomware trends, attack vectors, and the financial and operational impacts on targeted companies. By examining real-world case studies, we identify critical response strategies and highlight the effectiveness of Business Continuity Planning (BCP) and Disaster Recovery (DR) frameworks in minimizing downtime and data loss. Additionally, we explore innovations like immutable infrastructure and Virtual Desktop Infrastructure (VDI) as resilience measures. Through a detailed comparison of companies that paid ransoms versus those that refused, this paper underscores the financial and ethical challenges of ransomware response. Our findings suggest that robust, proactive defenses and recovery planning are essential in today's evolving threat landscape, enabling organizations to mitigate ransomware's impact without capitulating to attackers.

Keywords—Ransomware, cybersecurity, business continuity, disaster recovery, ransomware trends, cyber extortion.

I. INTRODUCTION

Ransomware has emerged as one of the most destructive forms of cyberattacks, targeting organizations of all sizes across industries. Attackers encrypt critical business data, demanding large ransom payments in exchange for decryption keys. The global average cost of ransomware attacks is rising, now exceeding millions of dollars ($4.88 Million) when considering both ransom payments and operational downtime, with a total global cost exceeding $9 Trillion.

This research paper explores how companies can survive ransomware attacks by analyzing case studies, attack vectors, and effective response strategies. It also emphasizes the importance of robust Business Continuity Planning (BCP) and Disaster Recovery (DR) measures, such as Virtual Desktop Infrastructure (VDI) and immutable systems, to enhance resilience.

Finally, we explore novel concepts and approaches to keep sensitive data like PII out of the hands of attackers by rethinking how data is handled in some industries.

II. THE IMPACT OF RANSOMWARE ON BUSINESSES AND ASSOCIATED ATTACK VECTORS

A. Financial Costs of Ransomware

Ransomware attacks have financially devastated many organizations, forcing some to pay millions in ransom to restore operations. Notable examples include Garmin [2], which paid around $10 million to recover from the WastedLocker ransomware attack, and CWT Global, [1] which paid $4.5 million following the Ragnar Locker attack.

Despite paying these large sums, companies still suffer operational downtimes. For Garmin, critical services like Garmin Connect and flyGarmin were disrupted for 4 to 5 days. Similarly, CWT Global restored operations within 48 hours of paying the ransom.

In some cases, the impact is catastrophic. In the case of Travelx (UK), the company was forced out of business after a ransomware attack decimated their business.

B. Operational Downtime and Recovery

Companies that refuse to pay the ransom often experience longer recovery times but develop stronger resilience. For instance, Norsk Hydro [3], a major aluminum producer, refused to pay the LockerGoga ransom and instead relied on backups to restore its systems. This decision led to several weeks of manual operations while systems were being rebuilt.

Similarly, Maersk, affected by the NotPetya ransomware, recovered without paying a ransom by restoring systems from backups, though it took the company 10 days to fully recover.

C. Common Ransomware Attack Vectors

Attackers use a variety of methods to breach organizations, with certain techniques and software being particularly vulnerable. Common methods include:

- Phishing Attacks: Many ransomware campaigns begin with phishing emails containing malicious links or attachments. Employees who click on these links unwittingly activate the ransomware.
- Exploiting Software Vulnerabilities: Ransomware like NotPetya and WannaCry leveraged vulnerabilities in Microsoft Windows systems, specifically the EternalBlue exploit. This exploit targeted vulnerabilities in the SMB protocol, allowing attackers to propagate quickly across networks.

- Remote Desktop Protocol (RDP) Attacks: Weak or compromised RDP credentials are frequently exploited by attackers to gain unauthorized access to systems.

With Windows operating systems being a primary target, attackers often exploit known vulnerabilities such as CVE-2017-0144, the SMBv1 vulnerability used in NotPetya.

III. NOTABLE RANSOMWARE TRENDS

A. Healthcare Industry

Healthcare providers are lucrative targets for ransomware due to the sensitivity and urgency of their data. Double extortion involves not only encrypting the data but also threatening to release patient information unless the ransom is paid. Triple extortion goes further by adding pressure through additional attacks, like DDoS, or contacting patients directly to create panic.

These tactics exploit the critical need to keep medical systems operational and patient data confidential, forcing healthcare providers to quickly resolve the situation, often by paying the ransom.

B. GenAI and RaaS

The emergence of Generative AI (GenAI) has accelerated the growth of Ransomware-as-a-Service (RaaS) by lowering technical barriers for cybercriminals. GenAI allows attackers with limited skills to use pre-built, AI-generated ransomware code, speeding up attack creation. It also helps generate convincing phishing emails or social engineering attacks, making the initial infection easier.

Furthermore, AI-driven automation aids in identifying vulnerabilities and expanding attack surfaces, making RaaS more scalable and accessible to a wider range of cybercriminals, increasing the frequency and complexity of attacks.

IV. ANALYSIS AND FINDINGS

A. Analysis Criteria

Incidents needed to meet a threshold:

- Confirmed ransomware incident through public relations / news announcements
- Incident duration/downtime needed to be known/measurable
- Sample sizes of the businesses who paid, and those who refused to pay, needed to be comparable to properly calculate any benefit in reduction of MTTR.

Once averages are determined, outliers can be further analyzed for specific situations or concerns.

B. Key Findings

1) Ransom Payments

Reported ransom payments for specific case studies. Only the known paid amounts are used for analysis of the average payment amount.

- CWT Global: $4.5 million [1]
- Garmin: Approximately $10 million (reported) [2]
- University of California, San Francisco (UCSF): $1.14 million [8]
- JBS USA: $11 million [7]
- Travelex: $2.3 million [29]
- University of Utah: $457,000 [18]
- Canon: Undisclosed (but likely significant) [17]
- Colonial Pipeline: $4.4 million [4]
- DCH Health System: Undisclosed (but paid ransom) [30] [52]
- Eurofins Scientific: Undisclosed (but paid ransom) [15]
- Sopra Steria: Undisclosed (but paid ransom) [21]
- Allied Universal: Undisclosed (but paid ransom) [22]
- Wood Ranch Medical: Did not pay; closed down [27]
- Hospitality Company (Unnamed, USA): Estimated millions [53]

2) Estimating the Average

To calculate the average ransom amount, I'll focus on the cases where the ransom amount is known:

- Total Ransom Known: $4.5M (CWT) + $10M (Garmin) + $1.14M (UCSF) + $11M (JBS) + $2.3M (Travelex) + $457K (University of Utah) + $2.3M (TravelX) + $4.4M (Colonial) = $36.097 million
- Number of Known Ransom Amounts: 8
- Average Ransom Amount: $36.097M / 8 = $4.512 million

C. Considerations

- Undisclosed Payments: Several companies paid a ransom but did not disclose the amount, so the actual average could be higher or lower depending on those cases.
- Large Payments Influence: High payments by companies like JBS USA ($11 million) and Garmin ($10 million) skew the average upward. [11]

D. Summary

The estimated average ransom paid by companies in these cases is approximately $4.5 million. This closely reflects other independent analysis which show the global average to be $4.88 million.

Other impacts such as businesses reputation, customer sentiment and business relationships, can have longer lasting impact.

V. BREAKDOWN OF TACTICS, TECHNIQUES AND PROCEDURES

Below is the relative distribution of attack tactics used. It should be noted that even when the tactic is often to exploit a vulnerability, the opportunity to do so often comes on the heels of a malicious link, phishing email (91%) [55] or other social engineering tactics (98%) [54].

- Phishing Emails: 15%
- Exploiting Software Vulnerabilities: 35%
- Remote Desktop Protocol (RDP) Attacks: 15%
- Supply Chain Attacks: 10%
- Social Engineering: 10%
- Embedded Malware: 15%

A. Commonly Exploited Software and Technologies

In the context of the ransomware attacks affecting the companies listed, specific pieces of software and technologies were commonly exploited, particularly those with known vulnerabilities. Here's a detailed look at the commonly exploited software:

1) *Windows Operating System*

- Description: Many ransomware attacks, including those involving NotPetya, exploit vulnerabilities in Windows OS.
- Common Vulnerabilities:
  - EternalBlue: An exploit developed by the NSA and leaked by the Shadow Brokers, which targets a vulnerability in Microsoft's implementation of the SMB protocol. [37]
  - CVE-2017-0144: The specific vulnerability in SMBv1 that EternalBlue exploits. [36]
- Examples: NotPetya, WannaCry.

2) *SMB Protocol (Server Message Block)*

- Description: A network file sharing protocol used by Windows. Vulnerabilities in SMB have been widely exploited by ransomware.
- Common Vulnerabilities:
  - CVE-2017-0144 (EternalBlue). [36] [37]
  - CVE-2017-0145: Another SMB vulnerability exploited by EternalRomance, used in NotPetya.
- Examples: NotPetya, WannaCry. [38]

3) *Microsoft Office and Macros*

- Description: Office macros have been used to deliver ransomware payloads through phishing emails.
- Common Vulnerabilities:
  - CVE-2017-0199: A vulnerability in Office that allowed remote code execution via specially crafted documents. [39]
- Examples: Locky, Dridex. [40]

4) *NotPetya Exploitation*

Exploited Vulnerabilities

- EternalBlue (CVE-2017-0144): Exploits a vulnerability in SMBv1. [36]
- EternalRomance (CVE-2017-0145): Another SMB exploit that targets a different vulnerability.[38]
- Mimikatz: A tool used to extract plaintexts passwords, hashes, PIN codes, and Kerberos tickets from memory. [42]
- Credential Dumping: Leveraged to spread laterally across networks using harvested credentials.

Typical Exploits: Initial Infection: Often through phishing emails or malicious updates, such as those seen in the MeDoc accounting software update (specifically in Ukraine). [41]

Spread Mechanism: Uses SMB vulnerabilities (EternalBlue and EternalRomance) to spread across networks.[36] [38]

Lateral Movement: Utilizes tools like Mimikatz to harvest credentials and move laterally within the network. [42]

Payload Delivery: Delivers the ransomware payload which encrypts files and renders systems inoperable. [42]

B. TTP Summary

The primary technology and software exploited in many of these ransomware attacks include vulnerabilities in the Windows operating system and the SMB protocol. NotPetya, in particular, leveraged SMB vulnerabilities extensively, exploiting both EternalBlue and EternalRomance. Understanding and addressing these vulnerabilities is critical for preventing similar ransomware attacks in the future.

VI. REFUSAL TO PAY AND THE IMPACT ON RECOVERY

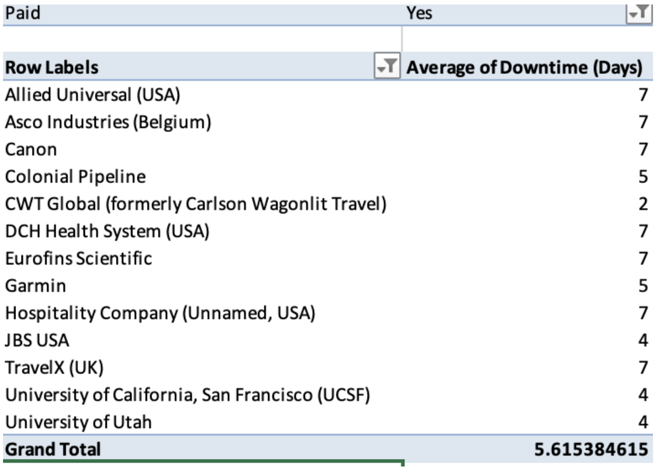
Companies that refuse to pay the ransom often experience longer recovery times but develop stronger resilience. For instance:

- Norsk Hydro, a major aluminum producer, refused to pay the LockerGoga ransom and instead relied on backups to restore its systems. This decision led to several weeks of manual operations while systems were being rebuilt. [3]
- Maersk, affected by the NotPetya ransomware, recovered without paying a ransom by restoring systems from backups, though it took the company 10 days to fully recover.
- Co-op (Federated Co-operatives Limited), gas and grocery chain across Western Canada. 500 stores were temporarily closed, with further supply chain impacts seen after opening. Cardlock out of service for a full month.

A. The Effect on Downtime of Paying a Ransom

1) *Average Downtime for Companies that Paid the Ransom*

Companies that paid the ransom faced an average downtime of 5.6 days, as shown in Fig 1.

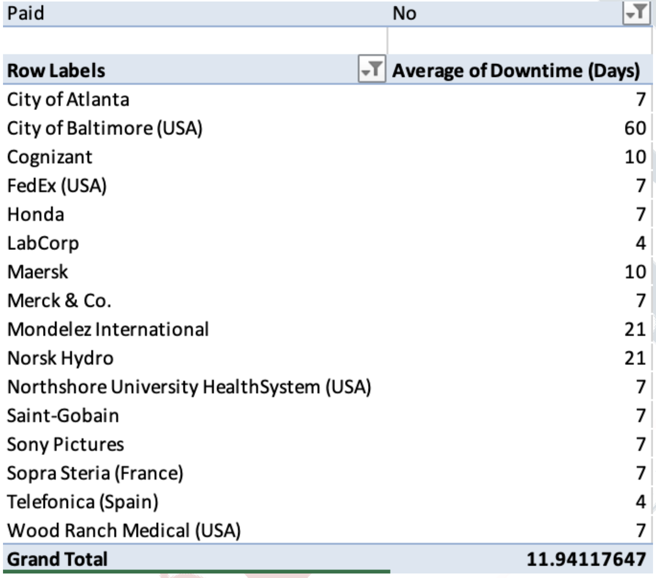


Paid	Yes
Row Labels	**Average of Downtime (Days)**
Allied Universal (USA)	7
Asco Industries (Belgium)	7
Canon	7
Colonial Pipeline	5
CWT Global (formerly Carlson Wagonlit Travel)	2
DCH Health System (USA)	7
Eurofins Scientific	7
Garmin	5
Hospitality Company (Unnamed, USA)	7
JBS USA	4
TravelX (UK)	7
University of California, San Francisco (UCSF)	4
University of Utah	4
Grand Total	**5.615384615**

Fig 1. Average downtime for companies which paid a ransom demand.

2) *Average Downtime for Companies that Refused to Pay the Ransom*

Companies that refused to pay generally experienced longer downtimes, with an average of 11.9 days, as shown in Fig 2.



Paid	No
Row Labels	**Average of Downtime (Days)**
City of Atlanta	7
City of Baltimore (USA)	60
Cognizant	10
FedEx (USA)	7
Honda	7
LabCorp	4
Maersk	10
Merck & Co.	7
Mondelez International	21
Norsk Hydro	21
Northshore University HealthSystem (USA)	7
Saint-Gobain	7
Sony Pictures	7
Sopra Steria (France)	7
Telefonica (Spain)	4
Wood Ranch Medical (USA)	7
Grand Total	**11.94117647**

Fig 2. Average downtime for companies which refused to pay a ransom demand.

3) *Ransomware Recovery Strategies*

NIST, CISA, ISACA, and the Ransomware Task Force collectively stress that effective ransomware resilience hinges on a comprehensive disaster recovery strategy, which includes frequent data backups, secure storage, network segmentation, and regular recovery drills. These elements ensure organizations can quickly restore critical operations without paying ransoms, ultimately reinforcing continuity and reducing the impact of ransomware attacks.

When considering the recommendations to recover from a ransomware incident, the average recovery time shown in Fig 2 clearly indicates that companies lack the recommended robust DR procedures that can be leveraged to deal with ransomware attacks, and that difficult decisions needs to be made to balance the cost involved in paying the ransom versus losses incurred by not doing so. The impact is that currently, companies are facing twice as long restoration times when choosing to not pay the ransom, which puts business owners in an extremely difficult position when faced with moral, ethical, legal and practical implications of these decisions. [32] [33] [34] [35]

B. Outliers

CDK Global, a software firm serving roughly 15,000 car dealerships across North America brought car sales to a halt. The outage lasted over 2 weeks. $25 Million was likely paid in ransom. [31].

The extended outage may imply that efforts were made to restore operations first, and when they were unsuccessful, ransom payment was eventually made. This classifies the scenario as before refusing to pay and complying with demands (which excludes this incident from statistical calculations).

Labcorp, which was his by SamSam ransomware in 2018, never paid the ransom and successfully recovered operations in just a couple days. While this initially sounds like a success story, investors would later sue the company in 2020 over lack of action taken to shore up its cyber defenses. [12].

C. Risk Transference Through Insurance

One very inconvenient finding is that risk transference as a strategy can fail completely, depending upon what entity launched the attack. In the case of Merck, who were hit with the NotPetya ransomware in 2017, no ransom was paid, and operations were restored through backups after nearly 2 weeks. However, upon filing insurance claims for coverage of the downtime and losses due to the incident, insurers argued the attack (attributed to Russia by the US, which Russia denied) was a warlike action and therefore classified as a "war exclusion" and would not be covered. This went back and forth for years in the courts, with a final agreement/settlement reached in early 2024. One must wonder if the legal costs involved eclipsed the cost of the downtime of the original incident. [43] [44]

VII. RECOMMENDATIONS FOR RESILIENCE AGAINST RANSOMWARE

A. Immutable Systems and Ephemeral Infrastructure

Adopting immutable systems and ephemeral infrastructure can significantly reduce the risk and impact of ransomware attacks. Systems that are stateless and easily replaceable prevent persistent infections. Ephemeral systems, which reset to a known good state at every login, enhance resilience by ensuring that faults do not propagate. Tools like Terraform and Ansible enable the automation of creating immutable infrastructure, ensuring that infrastructure remains consistent and can be replaced rather than repaired when compromised.

[45] [46]

B. Virtual Desktop Infrastructure (VDI)

VDI solutions, such as VMware Horizon and Citrix Virtual Apps and Desktops, allow organizations to deliver virtual desktops that can be reset to a clean state. By centralizing desktop management, VDI mitigates the risk of local malware infections, ensuring that any infected system can be quickly re-imaged. This approach also simplifies patching and security updates, further enhancing the resilience of desktop environments.

However, special attention needs to be paid to how data created during a VDI session is managed. While end of session actions should return the system to a clean state (and remove ransomware), data encrypted by ransomware would remain so. Recommended actions [47] would be to:

- Use a continuous data protection tool to make it possible to roll files back to their pre-encryption state.
- Restricting user permission to access only data that is necessary for them to do their jobs.
- Configure the user's web browsers as sandboxed virtual applications.

C. Business Continuity Planning (BCP) and Disaster Recovery (DR)

Having a robust Business Continuity Plan (BCP) and Disaster Recovery (DR) strategy is essential for minimizing downtime during a ransomware attack. Companies that regularly back up their data, segment their networks, and test their recovery plans are better positioned to recover without paying a ransom.

Key measures include:

- Regular, offline backups stored in separate, secure locations to avoid being encrypted alongside operational systems. [49]
- Network segmentation to limit the spread of ransomware, ensuring that critical systems are isolated from less secure parts of the network. [50]
- Multi-factor authentication (MFA) for critical systems to add a layer of protection beyond passwords.
- Regularly test 'recover from zero' scenarios. Ensure that your business continuity and disaster recovery process can rapidly bring critical business operations online from a zero functionality (all systems down) situation. Validate cross-team processes and technical procedures, including out-of-band employee and customer communications. [48]
- Print the required supporting, restoration-procedure documents required for recovery, including network diagrams, as attackers regularly destroy these documents. [48]

VIII. LESSONS FROM COMPANIES THAT SURVIVED RANSOMWARE

Organizations that have survived ransomware attacks demonstrate the importance of preparation and resilience. For example, Norsk Hydro refused to pay the ransom and restored operations through well-tested backup strategies, gaining praise for its transparency. Similarly, Maersk [5] recovered by using unaffected backups to restore its systems after the NotPetya attack, becoming a case study for effective incident response.

However, some companies chose to pay the ransom to expedite recovery. Garmin [2] and JBS USA paid millions to recover quickly, but this comes with risks. While paying a ransom may result in faster recovery, it encourages attackers to continue their operations, and there is no guarantee that decryption keys will work as promised.

In some cases, if the threat actor is affiliated with a Nation State engaged in other activities, paying a ransom may be illegal. [51]

IX. CONCLUSION

As ransomware attacks continue to evolve, businesses must prepare by investing in resilient systems and response strategies. Immutable systems, VDIs, data integrity tools, and robust BCP and DR measures are critical components of an organization's defense against ransomware.

Companies that survive ransomware attacks demonstrate that preparation is key in reducing downtime, but that most businesses are not prepared to effectively handle a ransomware attack without paying a ransom demand. Regular backups, tested recovery plans, and investing in resilient infrastructure can mitigate the damage caused by an attack and prevent long-term operational and financial harm. While paying a ransom may offer a short-term solution, it carries significant risks. Businesses should be encouraged to focus on proactive security measures to ensure they can recover quickly without resorting to paying attackers, especially if one day the option of paying a ransom itself is not a legal option.

REFERENCES

[1] J. Stubbs. "'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals." Reuters. https://www.reuters.com/article/world/us/payment-sent-travel-giant-cwt-pays-45-million-ransom-to-cyber-criminals-idUSKCN24W26O/ (accessed 07/24/2024).

[2] J. Tiddy. "Garmin begins recovery from ransomware attack." BBC. https://www.bbc.com/news/technology-53553576 (accessed 06/15/2024).

[3] P. Austin. "This Company Was Hit With a Devastating Ransomware Attack—But Instead of Giving In, It Rebuilt Everything." Time. https://time.com/6080293/norsk-hydro-ransomware-attack/ (accessed 06/21/2024).

[4] M. Kerner. "Colonial Pipeline hack explained: Everything you need to know." https://www.techtarget.com/whatis/

feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (accessed 05/10/2024).

[5] M. McQuade. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed 07/11/2024).

[6] L.H. Newman. “Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare.” Wired. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ (accessed 05/09/2024).

[7] “JBS: Cyber-attack hits world's largest meat supplier.” BBC. https://www.bbc.com/news/world-us-canada-57318965 (accessed 03/20/2024).

[8] J. Tiddy. “How hackers extorted $1.14m from University of California, San Francisco.” BBC. https://www.bbc.com/news/technology-53214783 (accessed 04/18/2024).

[9] R. Vanderford. “Insurers Say Cyberattack That Hit Merck Was Warlike Act, Not Covered.” WSJ. https://www.wsj.com/articles/insurers-say-cyberattack-that-hit-merck-was-warlike-act-not-covered-11675897657 (accessed 02/16/2024).

[10] C. Burgess. “Mondelez and Zurich’s NotPetya cyber-attack insurance settlement leaves behind no legal precedent.“ CSO Online. https://www.csoonline.com/article/574013/mondelez-and-zurich-s-notpetya-cyber-attack-insurance-settlement-leaves-behind-no-legal-precedent.html (accessed 05/02/2024).

[11] “2014 Sony Pictures hack.” Wikipedia. https://en.wikipedia.org/wiki/2014_Sony_Pictures_hack (accessed 03/23/2024).

[12] C. Osborne. “Investors sue LabCorp over security failures in light of data breach, ransomware attack.” ZDNet. https://www.zdnet.com/article/investors-sue-labcorp-for-failures-to-shore-up-security-in-light-of-data-breach-ransomware-attack/ (accessed 07/28/2024).

[13] E. Kovacs. “NotPetya Attack Costs Big Companies Millions.” Security Week. https://www.securityweek.com/notpetya-attack-costs-big-companies-millions/ (accessed 05/02/2024).

[14] M. Novinson. “Cognizant Breach: 10 Things To Know About Maze Ransomware Attacks.” CRN. https://www.crn.com/slide-shows/security/cognizant-breach-10-things-to-know-about-maze-ransomware-attacks (accessed 04/22/2024).

[15] D. Shaw. “Eurofins Scientific: Forensic services firm paid ransom after cyber-attack.” BBC. https://www.bbc.com/news/uk-48881959 (accessed 06/12/2024).

[16] J. Tidy. “Honda's global operations hit by cyber-attack.” BBC. https://www.bbc.com/news/technology-52982427 (accessed 03/20/2204).

[17] I. Ilascu. “Canon publicly confirms August ransomware attack, data theft.” Bleeping Computer. https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/ (accessed 02/20/2024).

[18] C. Cimpanu. “University of Utah pays $457,000 to ransomware gang.” ZDNet https://www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang/ (accessed 05/18/2024).

[19] D. Palmer. “NotPetya cyber attack on TNT Express cost FedEx $300m.” ZDNet. https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/ (accessed 03/28/2024).

[20] “2019 Baltimore ransomware attack.” Wikipedia. https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack (accessed 04/19/2024).

[21] L. Abrams. “French IT giant Sopra Steria hit by Ryuk ransomware.” Bleeing Computer. https://www.bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransomware/ (accessed 04/03/2024).

[22] L. Abrams. “Allied Universal Breached by Maze Ransomware, Stolen Data Leaked.” Bleeping Computer. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/ (accessed 05/13/2024).

[23] S. Adler. “**FBI Warns of DoppelPaymer Ransomware Attacks Targeting Critical Infrastructure.”** HIPAA Journal. https://www.hipaajournal.com/fbi-warns-of-doppelpaymer-ransomware-attacks-targeting-critical-infrastructure/ (accessed 07/21/2024).

[24] C. Cimpanu. “Telefonica Tells Employees to Shut Down Computers Amid Massive Ransomware Outbreak.” Bleeping Computer. https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/ (accessed 07/28/2024).

[25] “Hospitals Resume Accepting Patients After Malware Attack.” Security Week. https://www.securityweek.com/hospitals-resume-accepting-patients-after-malware-attack/ (accessed 06/24/2024).

[26] L. Pascu. “Aircraft Component Maker ASCO Hit by Ransomware, Shuts Down Global Production.” Bitdefender. https://www.bitdefender.com/en-us/blog/hotforsecurity/aircraft-component-maker-asco-hit-by-ransomware-shuts-down-global-production/ (accessed 04/22/2024).

[27] S. Adler. “Wood Ranch Medical Announces Permanent Closure Due to Ransomware Attack.” HIPAA Journal. https://www.hipaajournal.com/wood-ranch-medical-announces-permanent-closure-due-to-ransomware-attack/ (accessed 04/18/2024).

[28] “NorthShore University Health System Data Breach Affects More Than 340,000 People.” CBS News. https://www.cbsnews.com/chicago/news/north-shore-data-breach-affects-more-than-340000-people/ (accessed 06/28/2024).

[29] “Travelex boss breaks silence 17 days after cyber attack.” BBC. https://www.bbc.com/news/business-51152151 (accessed 07/28/2024).

[30] J. Davis. “DCH Health Faces Federal Lawsuit After 10-Day Ransomware Attack.” Tech Target. https://www.techtarget.com/healthtechsecurity/news/366595884/DCH-Health-Faces-Federal-Lawsuit-After-10-Day-Ransomware-Attack (accessed 06/25/2024).

[31] S. Lyngaas. “How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom.” CNN. https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html (accessed 7/12/2024).

[32] B. Fisher. M. Souppaya. W. Barker. K. Scarfone. “Ransomware Risk Management: A Cybersecurity Framework Profile.” NIST. https://www.nist.gov/publications/ransomware-risk-management-cybersecurity-framework-profile (accessed 6/17/2024).

[33] “#StopRansomware Guide.” CISA. https://www.cisa.gov/stopransomware/ransomware-guide 9accessed 6/16/2024).

[34] L. Wlosinski. “Ransomware Response, Safeguards and Countermeasures.” ISACA. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/ransome-response-safeguards-and-countermeasures (accessed 6/21/2024).

[35] “Combating the Ransomware Threat with a Cross-Sector Approach.” IST. https://securityandtechnology.org/ransom

waretaskforce/ (accessed 6/21/2024).

[36] "Windows SMB Remote Code Execution Vulnerability." Microsoft. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144 (accessed 5/24/2024).

[37] L. H. Newman. "The Leaked NSA Spy Tool That Hacked The World." Wired. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ (accessed 5/24/2024).

[38] "What you need to know about the WannaCry Ransomware." Security.com. https://www.security.com/threat-intelligence/wannacry-ransomware-attack (accessed 5/24/2024).

[39] "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows." Microsoft. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0199 (accessed 5/26/2024).

[40] I. Arghire. "Dridex Attacks Exploit Recent Office 0-Day." Security Week. https://www.securityweek.com/dridex-attacks-exploit-recent-office-0-day/ (accessed 5/26/2024).

[41] "Ukraine cyber-attack: Software firm MeDoc's servers seized." BBC. https://www.bbc.com/news/technology-40497026 (accessed 5/26/2024).

[42] "What is Mimikatz?" Sentinelone. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/mimikatz/ (accessed 5/27/2024).

[43] R. Vanderford. "Insurers Say Cyberattack That Hit Merck Was Warlike Act, Not Covered." WSJ. https://www.wsj.com/articles/insurers-say-cyberattack-that-hit-merck-was-warlike-act-not-covered-11675897657 (accessed 06/01/2024).

[44] K. Townsend. "Merck Settles NotPetya Insurance Claim, Leaving Cyberwar Definition Unresolved." Securityweek. https://www.securityweek.com/merck-settles-notpetya-insurance-claim-leaving-cyberwar-definition-unresolved/ (accessed 06/02/2024).

[45] "Immutable Backups and How They Mitigate Ransomware Attacks." Veritas. https://www.veritas.com/information-center/immutable-backups (accessed 05/11/2024).

[46] S. Pritchard. "Ransomware: All the ways you can protect storage and backup." ComputerWeekly. https://www.computerweekly.com/feature/Ransomware-All-the-ways-you-can-protect-storage-and-backup (accessed 5/11/2024).

[47] B. Posey. "Is VDI susceptible to ransomware threats? " https://www.techtarget.com/searchvirtualdesktop/tip/Is-VDI-susceptible-to-ransomware-threats {accessed 5/12/2024).

[48] M. Simos. "3 steps to prevent and recover from ransomware." Microsoft. https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/ (accessed 05/12/2024).

[49] M. H. Goh. "Disaster Recovery vs Ransomware Recovery: Why IT Disaster Recovery Need Both." BCM Institute. https://blog.bcm-institute.org/it-disaster-recovery/disaster-recovery-vs-ransomware-recovery-why-it-disaster-recovery-need-both {accessed 06/29/2024)

[50] F. Mahmood. "Using Network Segmentation to Combat Ransomware." ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/using-network-segmentation-to-combat-ransomware {accessed 06/29/2024).

[51] A. Schwartz. "The Path to Banning Ransomware Payments." Center For Cybersecurity Policy and Law. https://www.centerforcybersecuritypolicy.org/insights-and-research/the-path-to-banning-ransomware-payments {accessed 06/29/2024).

[52] "The DCH Ransomware Attack: A Teachable Moment in Cyber-History." Heimdal Security. https://heimdalsecurity.com/blog/dch-ransomware-attack/ (accessed 04/21/2024).

[53] "The State of Ransomware Attacks in the Hospitality Industry" Ironscales. https://ironscales.com/blog/ransomware-in-hospitality-industry/ (accessed 05/25/2024).

[54] C. Reed. "30 Social Engineering Statistics – 2023." Firewall Times. https://firewalltimes.com/social-engineering-statistics/ (accessed 04/23/2024).

[55] A. Eser. "Social Engineering Statistics: Phishing Dominates Cyber Attacks, Costs Millions." Worldmetrics. https://worldmetrics.org/social-engineering-statistics/ (accessed 08/01/2024).