Ransomware: Causes, Costs, and Solutions

Sydney Duong, Computer Information Systems
Mentor: Dr. Weijun Zheng
RSCA 2025

Introduction

Ransomware is now becoming the main threat in cybersecurity as it impacts business activities, government services, and personal users across the globe. Ransomware locks out users from their systems and data, holding them ransom until payment is made enabling the organization to regain access to their data and systems. A classic example could be when an employee boots up their workstation, only to find one file available to them, a payment demand with a deadline, and warnings that their data will be made public or sold on the dark web if the ransom is not paid. Ransomware not only causes financial loss, but also disrupts important activities and exposes confidential information, including company data and employees' personal data. Cybercrime damage costs are expected to grow by 15% this year, reaching $10.5 trillion USD by 2025.9 Companies globally are focusing on how to protect themselves from these attacks. They often invest in purchasing more security tools, when the simplest and most effective solution of making adjustments to the employees or their systems should be at their focus.

This project seeks to investigate the root causes of ransomware attacks over the past decade, analyze trends in cybersecurity spending, and assess the effectiveness of these investments in mitigating threats. By understanding these core dynamics, I hope to propose more effective and cost-efficient solutions for combating ransomware and safeguarding digital systems.

Objectives

This project seeks to:

1. Highlight trends in the rates of ransomware within the past couple years.
2. Identify the root causes, or initial attack vectors, of ransomware attacks.
3. Analyze trends in company spending on cybersecurity tools and their measure of effectiveness.
4. Propose practical and cost-efficient solutions to mitigating the risks of ransomware.

Methods

To address these objectives, my research will be based off the key reports published from leading cybersecurity companies and research, such as the Verizon 2024 Data Breach Investigations Report, the 2024 SonicWall Cyber Threat Report, the IBM Cost of a Data Breach Report 2024, the Crowdstrike 2024 Global Threat Report, the 2024 State of the Phish Report, and the 2020 Phishing Benchmark Global Report.

Data collection will be done on key metrics including Initial access methods (initial access refers to the first tactic that cyber criminals use to compromise an organization's system or data, including things such as phishing, weak passwords, and software vulnerabilities), financial losses from ransomware, and corporate spending on cybersecurity.

Visual data analysis with trend graphs and statistics will be created from sources mentioned above, as well as various sources listed in the resources section. These graphs illustrate the dynamics between ransomware incidents and the efficacy of company bought cybersecurity tools.

Findings

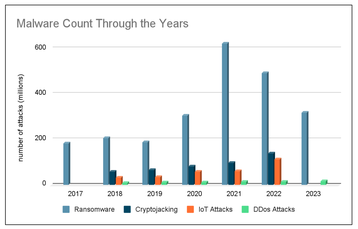

Figure 1: Malware Count Through the Years
Source 1: National University 101 Cybersecurity Statistics and Trends for 2024
Source 2: StationX Top +35 DDoS Statistics 2025

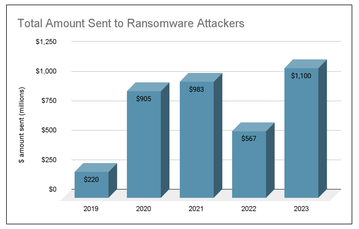

Figure 2: Total Amount Sent to Ransomware Attackers
Source: Chainalysis Ransomware Payments Exceed $1 2025

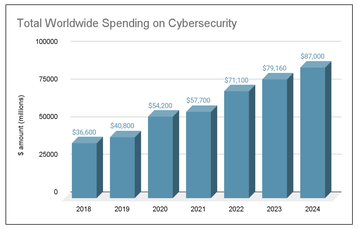

Figure 3: Total Worldwide Spending on Cybersecurity
Source: Statista Cybersecurity Spending Worldwide 2024

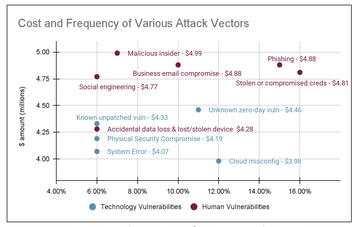

Figure 4: Cost and Frequency of Various Attack Vectors
Source: IBM Cost of a Data Breach Report 20245

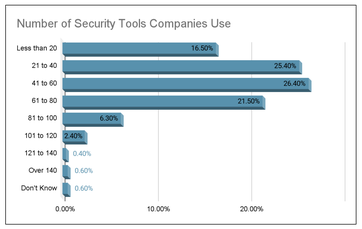

Figure 5: Number of Security Tools Companies Use
Source: IDC North American Security Tools and Vendors Consolidation Study: Insights on Product Consolidation Plans

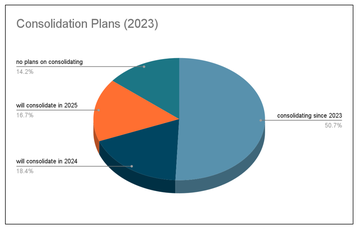

Figure 6: Consolidation Plans (2023)
Source: IDC North American Security Tools and Vendors Consolidation Study: Insights on Product Consolidation Plans

Analysis

In 2023, 317.6 million ransomware attacks were recorded, making it the third-highest year ever for the number of ransomware attacks. Even though the number has decreased since 2022, it should be noted that there has been a shift of focus in ransomware attacks from being high-scale to being more targeted and intentional. To highlight how ransomware is the most prevalent form of malware, refer to Figure 1. Ransomware by far has the highest volume of attacks. Cryptojacking has also become a rising concern, as the amount of people using cryptocurrency increases each year. This is further supported by the fact that 95% of attacks have a financial motive, with the rest consisting of espionage and political motives. Ransomware payments surpassed the record-breaking number of $1 billion in 2023 for the first time. Figure 2 highlights the general upwards trend in the amount spent on ransomware, showing the financial impact this issue brings. Next, Figure 3 reveals the worldwide trend that spending increases over time. Despite increasingly investing billions in cybersecurity annually, the effectiveness of this spending should raise some questions. We further see this trend played out through Figure 6. Human-based vulnerabilities (such as phishing, stolen or compromised credentials, malicious insiders, and business email compromise) are more costly and frequent over technical vulnerabilities (such as security misconfigurations, system errors, and unpatched vulnerabilities).

We see the redundancy of security tools with Figures 5 and 6. There are a wide array of tools that companies use for security, including, but not limited to: endpoint detection and response (EDR), extended detection and response (XDR), next-generation firewall (NGFW), security information and event management (SIEM), security service edge (SSE), and vulnerability/exposure management. Companies also can have multiple tools to account for mobile devices, cloud, and network security. This results in issues that reduces their effectiveness, such as (1) needing to manage dozens of security tools with overlapping functionalities and tenuous integrations, (2) staff productivity decreases with needing to switch between tools and correlate data, (3) alert fatigue rises as staff get a multitude of alerts from various sources, often overlapping with one another, and (4) information sharing between tools becomes complicated to the point where companies risk information siloing, preventing them from getting a comprehensive overview of their security posture and potentially delaying mediation time. More and more companies are planning to consolidate the number of tools they have, which shows that consolidation should be considered for increased efficiency.

Proposed Solutions

The most common vulnerabilities to ransomware are human-related, and that purchasing more security tools is not always effective,. Below are the proposed solutions to target the issue: What are the most proactive and effective measures organizations should take to lessen their risk to ransomware?

1. **Employee Training and Awareness Programs**. According to the 2024 Crowdstrike Global Threat Report6, the exploitation of valid credentials through human error (such as phishing, brute-force attacks, and insecure passwords) is one of the primary causes of a ransomware attack, therefore it is imperative to have employee education programs put in place. According Proofpoint's State of the Phish 2022, only 23% of employees were capable of recognizing phishing emails. After the training, 68% were able to recognize them.
2. **Enforcing Multi-Factor Authentication**. Applying MFA across all accounts reduces the risk of credential compromise. Threat actors are much more likely to target accounts without MFA, as passwords can be obtained through a multitude of ways. 123456 is still the most common password. Having MFA makes users 99% less likely to be hacked, even with a weak password.
3. **Performing Regular Patching and Updates**. IT teams should stay proactive with patching known vulnerabilities in all company software to hinder attackers utilizing them. Cybercriminals regularly seek out unpatched vulnerabilities, so regular patching would significantly reduce an organization's attack surface. Patching also helps comply with regulatory standards, such as GDPR, HIPPA, and PCI DSS)
4. **Security Tool Consolidation**. Not excessively spending on security tools provides companies with an opportunity to lessen operational costs and response time, while also increasing worker productivity. According to the IDC North American Security Tools Study, consolidating tools can save an average of 16% of cost, 20% of an analyst's time, reduce mean time to respond to 21%, and reduce remediation time by 19.5%.

Conclusion

The growing threat of ransomware necessitates a re-evaluation of strategies that organizations use to tackle cyberattacks and carry out security operations. Before spending more on security tools, it is important for companies to consider areas in which they can improve first. This means addressing the leading cause of ransomware attacks: human vulnerabilities. Implementing the solutions outlined above will help organizations effectively protect themselves against threats, and in turn any resulting consequences that come from data breaches. By learning from past incidents, it is clear that combining technical measures with human-centered initiatives is essential to combating ransomware, protecting sensitive data and business operations, and maintaining trust with all stakeholders.

References

2020 Phishing Benchmark Global Report. Terranova Security. (2020).

2024 Data Breach Investigations Report. Verizon Business. (2024).

2024 SonicWall Cyber Threat Report. Sonicwall.com. (2024).

2024 State of the Phish Report: Phishing Statistics & Trends. Proofpoint. (2025, January 2).

Borgeaud, A. (2024, June 18). Cybersecurity Spending Worldwide 2024. Statista.

Chainalysis Team. (2024, February 29). Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline. Chainalysis.

Cost of a Data Breach Report 2024 - IBM. ibm.com. (2024).

Crowdstrike 2024 Global Threat Report. crowdstrike.com. (2024).

Crowdstrike threat landscape: Apts & adversary groups. crowdstrike.com. (2025, January 3).

DBIR Report 2024 - Summary of Findings. Verizon Business. (2024b).

Morgan, S. (2024, November 18). Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. Cybercrime Magazine.

Multifactor Authentication. Cybersecurity and Infrastructure Security Agency CISA. (n.d.).

Prestianni, T. (2024, November 7). 101 cybersecurity statistics and Trends for 2024. National University.

Smith, G. (2024, December 11). Top +35 DDoS Statistics (2025). StationX.

Soltysik, M., & Kissel, C. (2024, April). North American Security Tools and Vendors Consolidation Study: Insights on Product Consolidation Plans. IDC.

Special Report: Mandiant M-Trends 2023. cloud.google.com. (2024, April).

U.S. Department of Justice Disrupts Hive Ransomware Variant. Office of Public Affairs | U.S. Department of Justice Disrupts Hive Ransomware Variant | United States Department of Justice. (2023, January 26).