

EVOLVING THREATS AND ADAPTIVE DEFENSES: A MULTI-SECTOR ANALYSIS OF RANSOMWARE IN THE UNITED STATES

 Majid Ziaei Nafchi¹;  Kristina Miska²

Prague University of Economics and Business, Faculty of Informatics and Statistics,
Department of Systems Analysis,
Nám. Winstona Churchilla 1938/4, 120 00 Praha 3-Žižkov, Czech Republic

e-mail: ¹majid.nafchi@vse.cz; ²miskaxristina@gmail.com

Abstract

Ransomware is an evolving cyber threat that continues to challenge organizations in the United States (U.S.). This study examines ransomware trends and defense strategies across healthcare, finance, and education from 2019 to 2023. Using a mixed-methods approach that combines survey data from 154 professionals with industry reports, the study identifies healthcare as the most vulnerable sector, finance as sustaining the highest losses, and education as facing the longest recovery times. The rise of ransomware-as-a-service and artificial intelligence (AI) has increased the complexity of attacks. Effective defense requires a coordinated approach to technical, organizational, and regulatory measures that build adaptive resilience.

Keywords

Cybersecurity; Organizational resilience; Artificial intelligence; Attack vectors.

Introduction

The exponential growth of digital infrastructures has revolutionized modern economies while simultaneously expanding the surface for cyberattacks. Among these, ransomware has emerged as one of the most disruptive and costly forms of cybercrime. Ransomware refers to malicious software that encrypts victims' data or systems, rendering them inaccessible until a ransom is paid (CISA, 2016). Over the last decade, ransomware has evolved from relatively simple malware into a sophisticated, profit-driven ecosystem that targets individuals, corporations, and governments alike.

In the U.S., ransomware incidents have risen at an alarming rate. The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reported a continuous increase in ransomware-related losses, which have reached hundreds of millions of dollars annually (FBI IC3, 2024). The country's high level of digitalization and concentration of valuable data make it a desirable target for attackers. Critical sectors, such as healthcare, finance, and education, have been disproportionately affected, experiencing not only financial and operational damage but also reputational harm and a loss of public trust.

While ransomware is a global phenomenon, its prevalence and impact in the U.S. warrant dedicated examination. Despite growing scholarly and policy attention (Saccone et al., 2025; Neprash et al., 2022; Yan & Khoei, 2025; Ahmed et al., 2022; McIntosh et al., 2023; Zetter, 2017), a lack of sector-specific analysis persists that simultaneously evaluates both the evolution of ransomware and the effectiveness of mitigation and recovery strategies.

The primary aim of this article was to analyze the recent evolution of ransomware incidents and evaluate the adaptive defense mechanisms implemented by organizations across critical U.S. sectors. It identifies key trends, vulnerabilities, and best practices for organizational defense. To achieve this, the research employed a mixed-methods design that integrated quantitative and qualitative data, as presented in the Methodology section, enabling a comprehensive assessment of ransomware trends and organizational defense strategies in the U.S. between 2019 and 2023, as discussed in the Results section, followed by their Discussion and Conclusion.

1 Literature Review

The evolution of ransomware has been marked by rapid technological sophistication and growing organizational vulnerability, transforming it from a limited cyber nuisance into a dominant global security threat. Early ransomware variants, such as the AIDS Trojan of 1989, employed rudimentary encryption and manual payment methods. Nevertheless, they laid the conceptual groundwork for what would become a lucrative form of cyber extortion (University of Tulsa, 2024). Over the past decade, ransomware has evolved into a well-organized, profit-driven ecosystem supported by specialized infrastructure, affiliate networks, and illicit marketplaces. Research shows that the shift toward professionalization and automation has blurred the boundaries between traditional cybercrime and cyberwarfare, with state-linked actors increasingly leveraging ransomware to pursue political and economic objectives (Greenberg, 2019). Together, these studies establish that ransomware is not simply a technical problem, but a socio-economic phenomenon driven by interdependent technological and human factors that amplify its global reach.

Saccone et al. (2025) provided a comprehensive empirical mapping of ransomware operations, identifying a recurring “blueprint” across 16,000 recorded incidents between 2020 and 2024. Their analysis revealed that most ransomware campaigns follow a consistent kill chain beginning with vulnerability exploitation and lateral movement, culminating in encryption and extortion. They distinguished between generalist gangs, such as LockBit and ALPHV, that apply complex multi-vector tactics across industries, and specialist actors focusing on specific sectors through social engineering or credential compromise. This structural differentiation underscores how ransomware has evolved beyond isolated attacks into an adaptive ecosystem that constantly reconfigures its techniques in response to defensive innovations. These insights reveal a pattern of strategic evolution in which ransomware groups continuously modify their tactics to sustain profitability and circumvent emerging security technologies.

Historical analyses further support this pattern of adaptive evolution. Zetter (2017) emphasized the significance of global outbreaks such as WannaCry and NotPetya, which revealed how ransomware could exploit systemic vulnerabilities to cause transnational disruption. These attacks demonstrated a convergence between ransomware and nation-state cyber operations, as code reuse and tool sharing made attribution more difficult. VMware (2020) noted that the COVID-19 pandemic accelerated the growth of ransomware by expanding digital dependency and increasing remote access vulnerabilities. The increased reliance on cloud storage, virtual private networks, and unsecured endpoints has offered fertile ground for threat actors, particularly in critical sectors such as healthcare and education. Taken together, these findings suggest that ransomware propagation is closely tied to global technological transitions, meaning that each wave of digital innovation introduces new attack surfaces that outpace existing safeguards.

The motives behind ransomware are equally diverse, ranging from financial profit to ideological activism. The rise of Ransomware-as-a-Service (RaaS) in the mid-2010s democratized access to sophisticated tools, allowing affiliates with limited technical skills to rent or license ransomware kits (Drake, 2022). This model fostered a commercialized

underground economy based on revenue sharing between developers and distributors. Meurs et al. (2024) advanced the theoretical understanding of ransomware economics by applying a signaling game framework to model double-extortion dynamics, in which attackers combine data encryption with exfiltration to enhance their leverage. Their results indicated that explicit defensive signaling, such as transparent resilience policies or visible investments in cybersecurity, can reduce attacker incentives by lowering the perceived likelihood of success. This complements the economic perspective outlined by Statista (2024), which estimated that ransom demands exceed \$4 million per incident in financial institutions, underscoring the rational, market-like nature of attacker decision-making. In summary, these perspectives demonstrate that ransomware thrives in a rationalized cybercriminal economy, where attackers respond strategically to market incentives and organizational defenses, underscoring the need for economically informed mitigation strategies.

Organizational and sectoral factors also play critical roles in shaping ransomware risk exposure. The healthcare sector is widely regarded as the most vulnerable due to its reliance on uninterrupted data access and the prevalence of outdated legacy systems (Neprash et al., 2022). Attacks on healthcare facilities often result in life-threatening delays and massive operational downtime, making them more likely to pay ransoms. Similarly, the education sector faces increasing pressure, as remote-learning platforms and limited IT funding create persistent security gaps (Bischoff, 2024). The financial industry, although technologically advanced, remains a prime target due to its potential for direct monetary gain and the interdependence of payment infrastructures (Statista, 2023). Saccone et al. (2025) confirmed that these three sectors account for the majority of ransomware incidents in the U.S., a trend corroborated by government and industry data, i.e. Cybersecurity and Infrastructure Security Agency (CISA). Synthesizing across sectors reveals that ransomware risk is a function of both technological exposure and institutional capacity, meaning that critical industries with high data value and limited redundancy face compounded vulnerability.

The growing complexity of the technological environment has also introduced new arenas of vulnerability. Yan & Khoei (2025) extended ransomware research into Internet of Things ecosystems, identifying exponential growth in attacks on connected devices between 2021 and 2023. Their proposed multilayered defense framework integrates AI-based intrusion detection, blockchain verification, and inter-organizational cooperation to build resilience. Their findings highlight that technical solutions alone are insufficient without organizational preparedness, employee awareness, and incident response planning. These insights align with the broader consensus in the cybersecurity literature that effective defense requires combining technological innovation with human and institutional adaptation, as introduced by the U.S. Department of Health and Human Services (HHS) and others (CISA, 2016; HHS, 2025). Collectively, these arguments underscore that effective ransomware mitigation must integrate technical, behavioral, and structural approaches to achieve lasting resilience.

Parallel advances in AI have influenced both attackers and defenders. Ahmed et al. (2022) explored ensemble learning models designed to counter adversarial evasion in ransomware detection. Their hybrid static-dynamic analysis—using Central Processing Unit, memory behavior, and network flow—enhances the robustness of malware classifiers against obfuscation techniques. Similarly, McIntosh et al. (2023) examined the application of generative AI in cybersecurity governance, risk, and compliance (GRC), showing that models such as GPT-4 can expedite the creation of security policies and automate compliance reporting. Together, these works underscore a dual narrative in which AI functions as both a weapon and a shield in the ransomware landscape. This synthesis reveals that AI's integration into cybersecurity is dialectical: it simultaneously empowers defense innovation and enhances the

sophistication of adversarial attacks, demanding continuous recalibration of defensive strategies.

While the technological sophistication of ransomware continues to evolve, the socio-organizational dimension remains a decisive factor. Human error, inadequate training, and insufficient resource allocation consistently emerge as primary enablers of successful attacks (Saleem et al., 2022). Studies indicate that awareness campaigns, periodic simulations, and integrated response planning significantly reduce susceptibility to phishing-based infiltration. Moreover, coordinated efforts among government agencies and private organizations, such as CISA's Pre-Ransomware Notification Initiative (CISA, 2023), demonstrate the efficacy of collective intelligence in pre-empting attacks. Synthesizing these insights suggests that ransomware defense effectiveness is determined not only by technological capability alone, but also by the maturity of organizational culture and interagency cooperation.

Taken together, existing literature portrays ransomware as a multifaceted threat defined by continuous adaptation and strategic innovation. Its evolution from isolated malware to an organized criminal enterprise reflects the broader dynamics of digital globalization and technological dependency. The research consensus converges on several key themes: the increasing professionalization of ransomware groups, the centrality of RaaS and affiliate structures, the critical role of AI in both attack and defense, and the enduring vulnerability of essential sectors. Nevertheless, gaps remain in cross-sectoral empirical analysis and in the integration of policy, organizational, and technical approaches. In synthesis, the reviewed literature demonstrates that the ransomware phenomenon is not only an outcome of advancing technology but also of uneven organizational readiness, signaling an urgent need for holistic, adaptive defense frameworks tailored to sector-specific contexts.

2 Methodology

The primary objective of this study was to investigate the evolution of ransomware incidents over recent years and to evaluate the adaptive defense mechanisms employed by organizations in critical U.S. sectors. This study employed a mixed-methods approach, combining quantitative and qualitative data, to assess ransomware trends and organizational defense strategies in the U.S. The U.S. is among the countries facing the highest number of ransomware attacks, and the data is more readily available due to higher incident reporting rates. Data collection was conducted between May and August 2024, focusing on the most recent five-year period, which covered ransomware incidents that occurred between 2019 and 2023. The 2019–2023 period was selected because it captures three structurally distinct ransomware phases: the pre-pandemic period, the COVID-19 digitalization shock (2020–2021), and the post-pandemic surge in ransomware-as-a-service and double-extortion tactics (2022–2023). The research focused on three critical sectors—healthcare, finance, and education—due to their high sensitivity to data and operational dependence on digital systems.

The objectives to achieve the main goal were to:

- Identify the most prevalent ransomware attack vectors and their sectoral variations.
- Assess organizational preparedness and recovery strategies in response to ransomware incidents.
- Evaluate the role of technological, human, and regulatory factors in mitigating ransomware impact.

To guide this investigation, two research questions (RQ) were formulated:

RQ1: What are the key trends in ransomware attacks affecting different sectors (healthcare, finance, and education) in the U.S. between 2019 and 2023?

RQ2: How do organizational strategies, including technical, human, and regulatory measures, contribute to resilience and recovery from ransomware incidents?

The authors of this study collected the primary data through an online survey administered to 154 cybersecurity professionals, information technology managers, and administrators working in the target sectors. The survey was created using Google Forms and consisted of 21 questions. It was made available online for three months (late May to late August 2024) and distributed through platforms such as LinkedIn, Facebook, and Reddit, with a target sample size of approximately 150 respondents. Respondents were selected through purposive sampling to ensure representation across organizational sizes and regional locations. The survey included both closed-ended and open-ended items measuring ransomware awareness, mitigation strategies, incident response practices, and perceived vulnerabilities.

Respondent anonymity was fully ensured throughout the data collection process. The survey was configured in Google Forms to prevent the storage of email addresses, IP addresses, or any other personally identifiable information, and participation was entirely voluntary. After collection, the data were exported into Microsoft Excel, where all closed-ended items were coded numerically and processed using descriptive statistical techniques to support the quantitative analysis. Open-ended responses were examined through a structured thematic coding approach to identify recurring themes related to attack vectors, mitigation practices, and recovery strategies. Coding was performed manually and supported by spreadsheet functions to organize categories and frequency counts. This procedure ensured a transparent and systematic analysis of both quantitative and qualitative components of the dataset.

Secondary data were drawn from public repositories and institutional sources, including reports from the CISA, the FBI, and Statista. These sources provided quantitative data on incident frequency, financial losses, and sector-specific impact.

Quantitative data were analyzed using descriptive statistics and cross-sectoral comparison to identify patterns in attack frequency, recovery duration, and ransom payment behavior. Qualitative responses were examined through thematic analysis to extract recurring themes related to organizational preparedness, employee behavior, and post-incident resilience. Triangulation between primary and secondary sources enhanced analytical validity, ensuring consistency between subjective perceptions and objective data.

By combining quantitative measurement with qualitative interpretation, this methodology provided a comprehensive understanding of ransomware dynamics and defense mechanisms. It enabled the study to capture both measurable outcomes and practitioner experiences, thereby ensuring a robust foundation for sector-specific analysis and comparative evaluation.

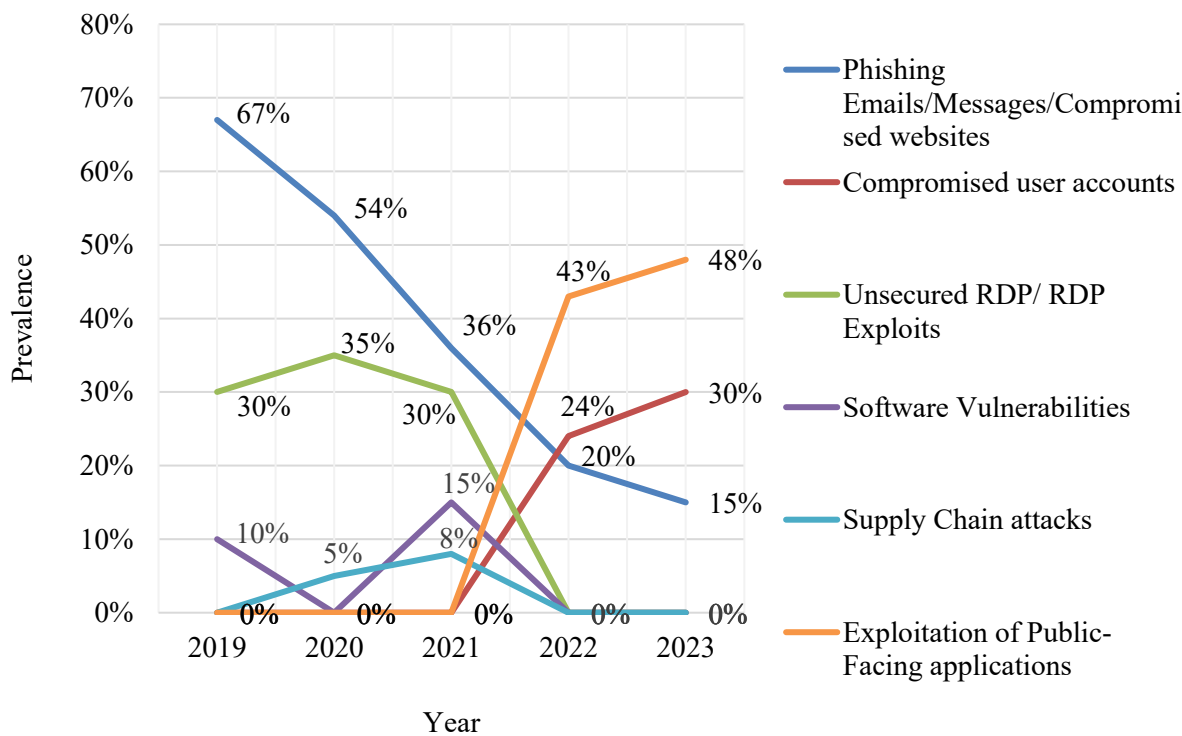
3 Results

The results first examine the evolution of ransomware attack vectors (RQ1), followed by sectoral differences in preparedness, recovery, and regulatory compliance (RQ2).

3.1 Answering RQ1 about Key Trends in Ransomware Attacks

The analysis identified six primary attack vectors used as entry points for ransomware across U.S. organizations, as illustrated in Figure 1. The percentages presented in Figure 1 represent the proportion of ransomware incidents in each year in which a given attack vector was identified as an initial access method. Because a single incident could involve more than one

entry point, each attack vector was coded independently as present or absent for every incident. As a result, the percentages do not sum to 100% within a given year and may exceed 100% when aggregated across years. Only the six most common attack vectors were included in Figure 1, which means that less frequent vectors were excluded. Accordingly, Figure 1 illustrates the prevalence of each vector across incidents rather than the relative distribution of mutually exclusive categories. Values of zero do not indicate complete absence but rather that the vector did not appear among the top-ranked vectors in those years. In 2019 phishing emails were the dominant vector, accounting for approximately 67% of reported incidents. Over time, however, the use of phishing, malicious messages, and compromised websites declined steadily, reaching around 15% by 2023. This reduction suggests a gradual shift in attackers’ strategies, likely driven by increased organizational awareness and improved filtering technologies.



Note: Attack vectors are not mutually exclusive. A single incident may involve multiple vectors.
Source: Own based on the online survey data and (FBI IC3, 2024)
Fig. 1: Trends in the most common attack vectors in the U.S. during the period of 2019-2023

Unsecured Remote Desktop Protocol (RDP) exploits emerged as a significant entry point in 2020, coinciding with the shift to remote work during the COVID-19 pandemic. These attacks peaked that year and gradually declined from 2021 onward as organizations adopted multi-factor authentication (MFA), stronger password policies, and stricter access controls.

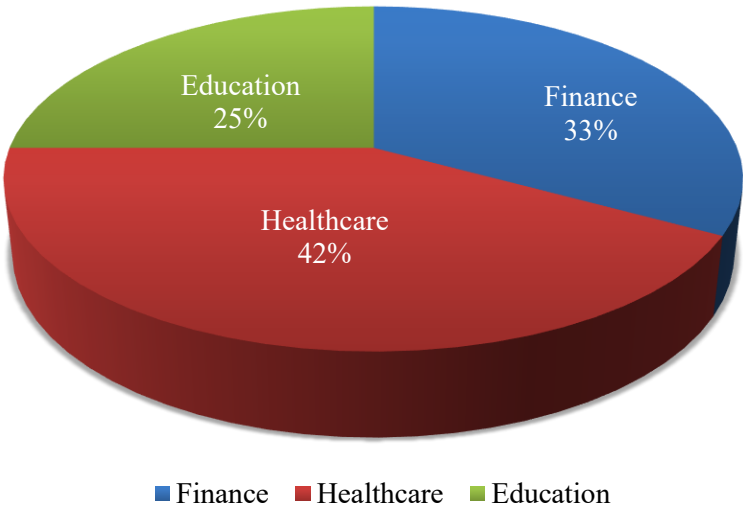
A notable trend that appeared in 2022 was the exploitation of public-facing applications, which rapidly became one of the most prevalent vectors. This method accounted for approximately 43% of reported incidents in 2022 and rose to about 48% in 2023. Attackers increasingly targeted exposed systems and cloud-based services, exploiting unpatched vulnerabilities and misconfigurations. The rise of this vector demonstrates the attackers’ growing technical sophistication and poses a heightened risk to sectors heavily dependent on digital infrastructure, such as healthcare and finance.

Software vulnerabilities also remained a consistent, though less dominant, vector throughout the study period. These weaknesses were exploited opportunistically but showed reduced prevalence over time, likely due to improved patch management and vulnerability assessment programs.

Supply chain attacks appeared most prominently in 2020 and 2021, marking a strategic evolution in ransomware deployment. Instead of targeting victims directly, attackers compromised third-party vendors or service providers to reach multiple downstream organizations.

Finally, compromised user accounts emerged as a significant vector beginning in 2022, accounting for roughly 24% of incidents, and increased to about 30% in 2023. This trend reflects attackers’ emphasis on credential theft, privilege escalation, and social engineering. The pattern aligns with the broader adoption of double-extortion tactics, in which attackers combine data encryption with theft of login credentials to increase leverage.

The financial impact of ransomware attacks over time shows that, while incident numbers fluctuate slightly year-to-year, total losses consistently increase. As shown in Figure 2, healthcare sector accounted for the largest share of incidents, averaging 42% of reported cases, reflecting its high operational dependency on continuous system availability and the prevalence of legacy infrastructure. Financial institutions account for 33% of incidents, consistent with their high data value and their attractiveness to extortion-driven attacks. Educational organizations account for 25% of reported cases, indicating lower attack frequency but not necessarily lower impact, as discussed in subsequent analyses of recovery and preparedness.



Source: Own based on the online survey data and (FBI IC3, 2024)
Fig. 2: Sectoral Distribution of Reported Cases averaged across the period of 2019–2023

The healthcare sector experienced extensive downtime averaging 18 days primarily due to outdated legacy systems and a lack of network segmentation. Finance reported the highest average ransom payments (USD 3.8 million per incident), with attacks increasingly leveraging double-extortion and data exfiltration schemes. Educational institutions experienced fewer incidents but faced prolonged recovery times due to limited IT budgets and decentralized network management. These results confirm distinct sectoral patterns in ransomware exposure, validating RQ1 by demonstrating that healthcare organizations experience the highest operational disruption, financial institutions bear the most considerable monetary losses, and education faces the slowest recovery processes.

3.2 Answering RQ2 about Organizational Strategies

Across all three sectors, respondents who reported using offline backups and formal incident response plans also reported substantially shorter recovery times. This pattern was strongest in the finance sector, where 79% of respondents indicated that backup systems were regularly tested and 90% reported having formal response procedures in place. In contrast, only 38% of healthcare and 29% of education respondents reported regular backup testing, which corresponds with the more extended downtimes observed in those sectors. These results indicate that recovery performance is closely linked to the maturity of preparedness measures.

Survey data further indicate that multi-factor authentication (MFA) and AI-supported monitoring tools reduced the prevalence of account-based compromise. Finance organizations, where 87% of respondents reported using MFA, had the lowest rate of compromised-user entries. In contrast, education, where only 42% reported MFA adoption, showed the highest growth in credential-based attacks. From a regulatory perspective, organizations subject to the CISA and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCI) reporting requirements reported faster coordination with external responders and earlier incident detection, reducing operational disruption. These patterns demonstrate that technology, human behavior, and regulatory oversight jointly shape recovery outcomes.

4 Discussion

This study evaluated ransomware dynamics and defense mechanisms across healthcare, finance, and education sectors in the U.S., guided by RQ1 and RQ2. The results show that ransomware evolution and organizational resilience are tightly connected: as attack vectors became more technically sophisticated after 2021, as shown in Figure 1 by the shift from predominantly phishing-based entry methods toward exploitation of public-facing applications, compromised user accounts, and supply chain attacks, organizations in the finance and healthcare sectors reporting higher preparedness and regulatory alignment experienced significantly better recovery outcomes.

Addressing RQ1, the results illustrate apparent sectoral differences in exposure and impact. Healthcare institutions face the highest attack frequency due to reliance on outdated systems and the ethical imperative of maintaining patient care continuity. Financial organizations, although technologically advanced, are often targeted for extortion due to the high value of their confidential data and the feasibility of ransom payments. Educational institutions remain the least prepared, constrained by limited resources and decentralized governance. These differences support earlier observations by Saccone et al. (2025) and Neprash et al. (2022) that organizational complexity and resource asymmetry are decisive factors in ransomware susceptibility. In synthesis, sectoral vulnerability is not uniform but contingent upon the intersection of technical exposure, economic value, and institutional resilience.

Addressing RQ2, the analysis revealed that effective defense depends on integrating technological, human, and regulatory measures. This conclusion is derived from 3 observed patterns:

1. respondents using MFA reported fewer account-based intrusions,
2. organizations with tested backups reported shorter downtime, and
3. organizations subject to CISA reporting frameworks reported faster incident coordination.

AI-based intrusion detection and automated response tools strengthen prevention, while employee awareness training and incident simulations reduce the likelihood of successful attacks. Compliance with CISA and FBI reporting frameworks facilitates faster recovery

through shared intelligence. Nevertheless, persistent underinvestment in human factors and inconsistent adherence to policy weaken overall resilience.

From a strategic perspective, the three objectives converge on a critical insight: ransomware defense must evolve from a reactive recovery approach to a proactive adaptation strategy. The study underscores the importance of a multi-layered security framework that incorporates early detection, sector-specific training, and interagency collaboration. Policies such as CISA (2022) and initiatives like CISA's Pre-Ransomware Notification Program (CISA, 2023) exemplify steps toward collective resilience but require broader institutional adoption. In synthesis, this discussion establishes that comprehensive protection against ransomware demands alignment between technical innovation, human capability development, and regulatory accountability. This triad defines the foundation of adaptive cybersecurity resilience.

A methodological limitation of this study concerns the classification of attack vectors. Because incidents could involve multiple initial access methods, the analysis treated attack vectors as non-mutually exclusive. This approach captures the presence of a vector within an incident but not the absolute frequency of its use across incidents. Consequently, percentages in Figure 1 reflect incidence proportions rather than exclusive distributions and may therefore exceed 100% when summed within a year. Additionally, less frequent attack vectors were excluded from the visualization, which limited the completeness of the annual distributions. These factors should be considered when interpreting longitudinal trends. Because purposive sampling was used to target cybersecurity professionals in critical sectors, the findings may not be statistically generalizable to all U.S. organizations; future research using larger, randomized samples could strengthen external validity.

Conclusion

This study examined the evolution of ransomware and the effectiveness of adaptive defense strategies across the healthcare, finance, and education sectors in the U.S. between 2019 and 2023, confirming that ransomware remains a complex and adaptive threat shaped by technological advancements, organizational capacity, and regulatory enforcement.

In response to RQ1, results revealed significant sectoral differences in ransomware exposure and impact. Healthcare organizations experienced the highest frequency of attacks and operational disruptions due to their legacy infrastructure and limited segmentation capabilities. Financial institutions sustained the most significant financial losses, reflecting both the value of their data and their ability to pay ransoms. Educational institutions, although less targeted, exhibited the most extended recovery periods due to underfunding and decentralized governance. These findings affirm that sectoral vulnerability is context-specific, influenced by the interplay of technical, economic, and institutional factors.

In response to RQ2, the analysis shows that organizations with MFA, tested backups, formal incident response plans, and regulatory reporting obligations experienced shorter downtimes and lower operational disruption than those without these controls. These relationships were most pronounced in the finance sector and weakest in education, demonstrating that cybersecurity resilience is measurable and sector-dependent.

Overall, the research achieves its objectives by identifying prevalent attack vectors, examining preparedness and recovery strategies, and evaluating the interdependence of technological, human, and regulatory defenses. The findings extend the current understanding of ransomware resilience by emphasizing that cybersecurity maturity cannot be achieved solely through technology—it must be institutionalized through governance, culture, and collaboration. The principal contribution of this study lies in its sector-level comparison of ransomware impacts

and its integration of practitioner survey data with institutional reporting, providing a multidimensional view of organizational cyber resilience.

Future research should build on these insights by conducting longitudinal studies that assess the evolution of ransomware tactics beyond 2023, as well as exploring the role of emerging technologies, such as quantum encryption and generative AI, in reshaping cyber defense. Strengthening partnerships between public agencies, private institutions, and academia will be essential to developing sustainable, adaptive defense frameworks capable of meeting the evolving ransomware threat landscape. In addition to longitudinal and technological extensions, qualitative case-study research would provide valuable insight into how organizational decision-making, leadership culture, and operational constraints shape ransomware resilience and recovery. In-depth interviews with security managers, IT staff, and executives could help explain why similar technical controls produce different outcomes across sectors, complementing the quantitative patterns identified in this study.

These conclusions are derived directly from sectoral comparisons of preparedness measures, recovery outcomes, and regulatory compliance observed in the survey and secondary data.

Acknowledgements

This article was supported by the institutional support fund for the long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the Prague University of Economics and Business (IP400040) and the project IG 409035.

References

- Ahmed, U., Lin, J. C.-W., & Srivastava, G. (2022). Mitigating adversarial evasion attacks of ransomware using ensemble learning. *Computers and Electrical Engineering*, 100, 107903. <https://doi.org/10.1016/J.COMPELECENG.2022.107903>
- Bischoff, P. (2024). *On average, US schools & colleges lose \$500K per day to downtime from ransomware attacks*. Comparitech. <https://www.comparitech.com/blog/information-security/school-ransomware-attacks/>
- CISA. (2016). *Protecting Your Networks from Ransomware*. Cybersecurity & Infrastructure Security Agency. <https://www.cisa.gov/resources-tools/resources/protecting-your-networks-ransomware>
- CISA. (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf
- CISA. (2023). JCDC Cultivates Pre-Ransomware Notification Capability. Cybersecurity & Infrastructure Security Agency. <https://www.cisa.gov/news-events/alerts/2023/03/23/jcdc-cultivates-pre-ransomware-notification-capability>
- Drake, V. (2022). *The History and Evolution of Ransomware Attacks*. Flashpoint. <https://www.flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/>
- FBI IC3. (2024). *Federal Bureau of Investigation Internet Crime Report 2023*. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3). https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf
- Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday. ISBN 978-0385544412.

- HHS. (2025). The U.S. Department of Health & Human Services. <https://www.hhs.gov/>
- McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, 134, article 103424. <https://doi.org/10.1016/J.COSE.2023.103424>
- Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. *Computers & Security*, 138, 103670. <https://doi.org/10.1016/J.COSE.2023.103670>
- Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, 3(12), e224873. <https://doi.org/10.1001/jamahealthforum.2022.4873>
- Saccone, F., Melillo, P., Sgueglia, A., Di Sorbo, A., & Visaggio, C. A. (2025). The ransomware blueprint: Attack patterns and strategic variations across gangs. *Journal of Information Security and Applications*, 95, 104264. <https://doi.org/10.1016/J.JISA.2025.104264>
- Saleem, J., Islam, R., Kabir, M. A. (2022). The Anonymity of the Dark Web: A Survey. *IEEE Access*, 10, 33628–33660. <https://doi.org/10.1109/ACCESS.2022.3161547>
- Statista. (2023). *Estimated amount of ransom demanded from U.S. healthcare organizations from 2019 to 2023 YTD*. <https://www.statista.com/statistics/1422162/us-healthcare-ransom-estimated-demanded/>
- Statista. (2024). *Average amount of cyber ransom payments at organizations in the United States in 2023, by industry*. <https://www.statista.com/statistics/1465613/average-ransom-payment-us-by-industry/>
- University of Tulsa. (2024). *Famous Ransomware Attacks in History*. <https://online.utulsa.edu/blog/famous-ransomware-attacks-in-history>
- VMware. (2020). *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted*. VMware Security Blog. <https://blogs.vmware.com/security/2020/04/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted.html>
- Yan, P., & Khoei, T. T. (2025). Securing the internet of things: A comprehensive review of ransomware attacks, detection, countermeasures, and future prospects. *Franklin Open*, 11, article 100256. <https://doi.org/10.1016/J.FRAOPE.2025.100256>
- Zetter, K. (2017). *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*. Wired. <https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/>

VYVÍJEJÍCÍ SE HROZBY A ADAPTIVNÍ OBRANA: MULTISEKTOROVÁ ANALÝZA RANSOMWARU VE SPOJENÝCH STÁTECH

Ransomware je neustále se vyvíjející kybernetická hrozba, která představuje výzvu pro organizace ve Spojených státech (USA). Tato studie zkoumá trendy v oblasti ransomwaru a obranné strategie ve zdravotnictví, financích a vzdělávání v letech 2019 až 2023. Pomocí kombinované metody, která spojuje údaje z průzkumu mezi 154 odborníky s odvětvovými zprávami, studie identifikuje zdravotnictví jako nejzranitelnější sektor, finance jako sektor s nejvyššími ztrátami a školství jako sektor s nejdelší dobou zotavení. Vzestup ransomwaru jako služby a umělé inteligence (AI) zvýšil složitost útoků. Účinná obrana vyžaduje koordinovaný přístup k technickým, organizačním a regulačním opatřením, která budují adaptivní odolnost.

SICH WANDELNDE BEDROHUNGEN UND ADAPTIVE ABWEHRMECHANISMEN: EINE BRANCHENÜBERGREIFENDE ANALYSE VON RANSOMWARE IN DEN USA

Ransomware ist eine sich ständig weiterentwickelnde Cyberbedrohung, die US-amerikanische Organisationen weiterhin vor große Herausforderungen stellt. Diese Studie untersucht Ransomware-Trends und Abwehrstrategien im Gesundheitswesen, Finanzsektor und Bildungswesen von 2019 bis 2023. Anhand von Umfragedaten von 154 Fachkräften und Branchenberichten wird das Gesundheitswesen als am stärksten gefährdet, der Finanzsektor als der mit den höchsten Verlusten und der Bildungssektor als der mit den längsten Wiederherstellungszeiten konfrontiert identifiziert. Der Aufstieg von Ransomware- als Dienstleistung und künstlicher Intelligenz (AI) hat die Komplexität der Angriffe erhöht. Eine effektive Abwehr erfordert koordinierte technische, organisatorische und regulatorische Maßnahmen zum Aufbau adaptiver Resilienz.

EWOLUUJĄCE ZAGROŻENIA I ADAPTACYJNE MECHANIZMY OBRONNE: WIELOSEKTOROWA ANALIZA OPROGRAMOWANIA RANSOMWARE W STANACH ZJEDNOCZONYCH

Oprogramowanie ransomware to ewoluujące cyberzagrożenie, które wciąż stanowi wyzwanie dla organizacji w Stanach Zjednoczonych (USA). Niniejsze badanie analizuje trendy dotyczące oprogramowania ransomware i strategie obronne w sektorze służby zdrowia, finansów i edukacji w latach 2019–2023. Wykorzystując podejście oparte na metodzie mieszanej, łączącej dane z badań przeprowadzonych wśród 154 specjalistów z raportami branżowymi, służbę zdrowia zidentyfikowano w badaniach jako sektor najbardziej narażony, sektor finansowy jako sektor ponoszący największe straty, a sektor edukacji jako sektor o najdłuższym czasie przywracania sprawności. Rozwój oprogramowania ransomware jako usługi i sztucznej inteligencji (AI) zwiększył złożoność ataków. Skuteczna obrona wymaga skoordynowanego podejścia do rozwiązań technicznych, organizacyjnych i regulacyjnych w celu zbudowania adaptacyjnej odporności.