Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(RESEARCH ARTICLE)

Escalating Ransomware Threats in the United States: Trends, Economic Impacts and Policy Responses (2020–2024)

Seun Adeniran [1,*], Michael Ariyo [2], Francis Dumbili [3] and Onyinye Uzoka [4]

[1] *Department of Engineering, Tennessee State University Nashville, USA.*
[2] *College of Science, Health and Pharmacy, Roosevelt University Chicago, USA.*
[3] *Faculty of Law, Business and Tourism, University of Sunderland, UK.*
[4] *Hertfordshire Business School, University of Hertfordshire, UK.*

Magna Scientia Advanced Research and Reviews, 2025, 15(02), 119-133

Publication history: Received 27 October 2025; revised on 04 December 2025; accepted on 06 December 2025

Article DOI: https://doi.org/10.30574/msarr.2025.15.2.0148

Abstract

Ransomware attacks have emerged as one of the most disruptive cyber threats to the United States economy over the past five years. This study examines trends, economic impacts, and policy responses to ransomware incidents from 2020 to 2024, integrating data from the FBI's Internet Crime Complaint Center (IC3), Chainalysis, and other cybersecurity intelligence sources. Results indicate a sharp escalation in ransomware-related financial losses, rising from approximately $412 million in 2020 to over $1.6 billion in 2023, with notable sectoral vulnerabilities in healthcare, critical infrastructure, and government services. Statistical analysis reveals a moderate positive correlation ($r \approx 0.58$) between reported incidents and ransom payments, highlighting the sustained profitability driving criminal activity despite a decline in total complaints in 2023. The study further evaluates the effectiveness of policy interventions, including Executive Order 14028, sector-specific mitigation strategies, and public-private collaborations, identifying persistent gaps in ransomware preparedness and incident response. Findings underscore the urgent need for coordinated economic, regulatory, and technical measures to reduce ransomware exposure and strengthen cybersecurity resilience. This research contributes to a data-driven understanding of ransomware dynamics and informs evidence-based policy design for mitigating economic and societal risks in the United States.Keywords: Cybercrime; Cryptocurrency; Operational resilience; Sectoral vulnerability; Incident reporting; Ransomware-as-a-Service(RaaS)

Keywords: Digital Extortion; Cybersecurity; Operational Disruption Costs; Indicence Disclosure Compliance; Critical Infrastructure Protection

1. Introduction

Over the past decade, ransomware has emerged as one of the most destructive and financially consequential forms of cybercrime. Characterized by malicious software that encrypts victims' data and demands payment, often in cryptocurrency, for decryption, ransomware represents the convergence of traditional extortion tactics and modern digital vulnerabilities (Europol, 2023). Although ransomware is a global threat, the United States remains disproportionately affected, both in the frequency of attacks and in the magnitude of financial and operational losses (Federal Bureau of Investigation, FBI, Internet Crime Complaint Center ,IC3, 2024). This disproportionate burden reflects not only the nation's economic prominence and digital integration but also the attractiveness of U.S. institutions as high-value targets due to their extensive data assets and dependence on networked operations (Cybersecurity and Infrastructure Security Agency, CISA, 2023).

* Corresponding author: Seun Adeniran

Ransomware attacks in the U.S. have evolved significantly in both sophistication and organization. Early attacks in the 2010s were typically opportunistic, targeting individuals through spam emails or malicious attachments. However, since 2020, attackers have shifted toward "big game hunting", a strategy that focuses on large enterprises, hospitals, educational institutions, and local governments capable of paying substantial ransoms (Symantec, 2022). These campaigns are often conducted by well-structured criminal enterprises operating under the "Ransomware-as-a-Service" (RaaS) model, in which malware developers lease their code to affiliates in exchange for a share of ransom profits (Chainalysis, 2024). This service-based model has lowered the barrier to entry for cybercriminals and created a thriving underground economy, making ransomware both scalable and resilient to enforcement actions.

Data from official and independent sources underscore the scale of the crisis. According to the FBI IC3 (2024), reported ransomware complaints in the United States rose from 2,474 in 2020 to 3,156 in 2024, representing a 27.6% increase. Financial losses reported to IC3 also expanded, with adjusted losses exceeding $59.6 million in 2023, a figure that under-represents the true economic toll due to chronic underreporting by victims. Chainalysis (2024), which tracks cryptocurrency ransom payments through blockchain analysis, estimated that global ransomware payments reached $1.25 billion in 2023, the highest ever recorded. This divergence between official complaint data and blockchain-tracked payments illustrates a persistent data gap in national cyber incident reporting and highlights the need for multi-source monitoring frameworks.

The impacts of ransomware extend beyond immediate financial costs. Victimized organizations frequently experience operational downtime, reputational damage, data loss, and disruptions to critical services (Anderson et al., 2022). For example, ransomware attacks on hospitals have delayed patient care, while those on municipal governments have disrupted public services ranging from emergency response to school operations (KPMG, 2024). These systemic effects underscore that ransomware is not merely a cybersecurity issue but a national security and economic resilience concern. In sectors such as healthcare and education, where legacy systems and limited cybersecurity budgets prevail, the risk exposure remains particularly acute (CISA, 2024).

From a policy standpoint, the U.S. government has made notable strides in addressing the ransomware epidemic. Executive Order 14028 (2021) on "Improving the Nation's Cybersecurity" laid the groundwork for implementing zero-trust architectures and enhancing software supply chain security. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), enacted in 2022, mandates that critical infrastructure operators report cyber incidents within 72 hours and ransom payments within 24 hours (Department of Homeland Security, DHS, 2022). In parallel, the establishment of the Joint Ransomware Task Force (JRTF) in 2023 has facilitated coordination between the Federal Bureau of Investigation, CISA, and the U.S. Treasury to trace cryptocurrency flows and disrupt illicit networks. However, despite these developments, enforcement challenges, fragmented reporting mechanisms, and limited international cooperation continue to hinder comprehensive mitigation efforts (Harrell, 2023).

Academic literature on ransomware reflects an increasing interest in its economic, behavioral, and policy dimensions. Earlier research focused largely on the technical mechanisms of encryption, decryption, and malware propagation (Richardson an North, 2017), whereas recent studies have expanded to encompass the macroeconomic implications, including business continuity, insurance costs, and public trust in digital systems (Anderson et al., 2022; Prieto et al., 2023). Moreover, scholars have begun to examine how cryptocurrency ecosystems facilitate the ransomware economy by providing semi-anonymous payment channels and laundering opportunities (Chainalysis, 2024; Europol, 2023). Despite the progress in empirical understanding, a gap remains in synthesizing these diverse strands of evidence, particularly in connecting national incident data, financial analytics, and policy outcomes within a single review framework.

This paper therefore seeks to bridge that gap by synthesizing the trends, economic impacts, and policy responses to ransomware in the United States between 2020 and 2024. Drawing on data from the FBI IC3, Chainalysis, CISA, and peer-reviewed literature, it offers a consolidated picture of how ransomware has evolved during this critical period. Specifically, the paper traces the annual trajectory of ransomware complaints and losses; analyzes the divergence between reported and actual ransom payments; and evaluates the effectiveness of major U.S. policy interventions aimed at mitigating ransomware risks. By providing an integrated analysis of technical, economic, and institutional factors, this study contributes to ongoing debates on cyber resilience, information policy, and digital governance. The findings are intended to guide policymakers, cybersecurity professionals, and researchers in developing evidence-based strategies that enhance both national cybersecurity readiness and organizational recovery capacity. In doing so, the paper underscores that ransomware resilience is not solely a matter of technology, it is an outcome of coherent policy design, cross-sector collaboration, and sustained public–private engagement.

2. Methods

2.1. PRISMA Review Protocol

This review adhered to the PRISMA 2020 guidelines (Page et al., 2021), ensuring that the methodology was both transparent and reproducible. The objective was to systematically identify, examine, and synthesize empirical and policy-focused research concerning ransomware trends, economic consequences, and mitigation strategies within the United States from 2020 to 2024. The sources for this review included peer-reviewed academic publications, government and institutional reports, as well as industry white papers, all assessed against established inclusion criteria.

2.2. Search Strategy

A comprehensive search was carried out across five prominent electronic databases: Scopus, Web of Science, IEEE Xplore, ScienceDirect, and Google Scholar, covering the period from January 2020 to September 2024. The search strategy utilized a combination of controlled vocabulary and free-text terms related to ransomware and U.S. cybersecurity policy, including: "ransomware," "crypto-extortion," "ransomware-as-a-service," "United States," "U.S.," "America," "cybersecurity policy," "economic impact," "critical infrastructure," "incident reporting," and "law enforcement response." This process was supplemented by manual screening of major journals (Computers and Security, Journal of Cybersecurity, Government Information Quarterly, Policy & Internet) and by consulting official datasets from sources such as the FBI IC3, CISA, and Chainalysis. Additionally, the reference lists of relevant publications were examined to identify further eligible studies.

2.3. Eligibility Criteria

To maintain analytical consistency, studies had to meet the following inclusion criteria:

- **Temporal scope:** Published between January 2020 and September 2024.
- **Geographical focus*:*** Centered on the United States or reporting disaggregated U.S. data.
- **Topical relevance*:*** Examined ransomware frequency, costs, prevention, or policy responses.
- **Document type*:*** Peer-reviewed empirical or conceptual articles, official agency reports, or recognized industry analyses (e.g., KPMG, Symantec, IBM Security).
- **Language*:*** English.

Exclusion criteria included non-U.S. case studies, duplicate or derivative publications, technical studies without socioeconomic or policy context, and non-credible gray literature such as blogs or promotional content.

2.4. Screening and Selection Process

All titles and abstracts were thoroughly screened. The initial search returned 1,242 records. After duplicate removal, 1,018 unique records remained. Title and abstract screening excluded 772 items, leaving 246 articles for full-text assessment. Following detailed review, 67 publications met the eligibility criteria, and an additional five government or industry reports were identified through manual searches. The final synthesis therefore included 72 sources (Table 1).

2.5. Data Extraction and Analysis

Data from included sources were extracted into a structured matrix comprising the following fields:

- **Bibliographic information** (author, year, source, and publication type).
- **Focus area** (trends, economic impacts, or policy/response measures).
- **Methodology** (quantitative, qualitative, or mixed methods).
- **Sectoral scope** (healthcare, education, finance, government, etc.).
- **Key findings** (statistical indicators, policy insights, or economic estimates).

Descriptive statistics were generated to summarize publication patterns and topical distribution. Quantitative trends (e.g., incident counts and financial losses) were triangulated against IC3 and Chainalysis datasets, while qualitative policy insights were narratively synthesized.

2.6. Quality Assessment

The methodological rigor of empirical studies was evaluated using a modified Critical Appraisal Skills Programme (CASP) checklist. Each paper was rated on relevance, data transparency, validity of analysis, and replicability. Government reports were assessed for source authority, documentation of data sources, and disclosure of assumptions.

2.7. Limitations of the Study

While this paper synthesizes diverse datasets, limitations include potential underestimation of incidents due to reporting gaps and variability in cost accounting across sectors. Future research should incorporate longitudinal, multi-sectoral datasets and explore the effectiveness of evolving policy interventions. Interdisciplinary studies integrating technical, economic, and organizational perspectives are crucial for developing adaptive and resilient strategies against ransomware threats.

3. Results and Trend Analysis

A total of 72 sources met the inclusion criteria for synthesis, comprising 38 peer-reviewed journal articles, 29 government or institutional reports, and 5 industry white papers published between 2020 and 2024. Table 1 presents the distribution of these sources by publication type, methodological approach, and thematic focus.

Table 1 Summary Characteristics of Included Studies (n = 72

Category	Subcategory	Number of Studies	Percentage (%)
Publication Type	Peer-reviewed journal articles	38	52.8
	Government/agency reports (FBI, CISA, GAO, DHS, NSA)	29	40.3
	Industry white papers (KPMG, IBM, Symantec, Chainalysis, Palo Alto Networks)	5	6.9
Methodological Approach	Quantitative (data-driven)	28	38.9
	Qualitative (policy or case analysis)	31	43.0
	Mixed-methods	13	18.1
Thematic Focus	Trend analysis (incident rates, typologies)	22	30.6
	Economic impact and cost assessment	26	36.1
	Policy response and institutional resilience	24	33.3
Sectoral Coverage	Healthcare	16	22.2
	Education	9	12.5
	Government/public sector	18	25.0
	Finance and insurance	11	15.3
	Critical infrastructure (energy, water, transport)	10	13.9
	Cross-sectoral/general	8	11.1

Note. Percentages may not sum to 100 due to rounding. Data compiled from peer-reviewed and grey literature included in the final synthesis.

3.1. Temporal Trends in Ransomware Incidents (2020–2024)

Ransomware incidents in the United States have exhibited fluctuating yet intensifying patterns between 2020 and 2024. Data reported by the FBI's Internet Crime Complaint Center (IC3) reveal a persistent upward trend, with only a brief decrease in 2022. Overall, ransomware complaints rose from 2,474 in 2020 to 3,156 in 2024, an increase of roughly 28%. This escalation appears closely tied to the growth of the ransomware-as-a-service (RaaS) ecosystem, which has lowered the barrier to entry for threat actors and enabled the targeting of critical infrastructure. Notably, 2021 saw a

sharp surge in incidents correlated with major attacks on organizations such as Colonial Pipeline and JBS Foods, which in turn prompted significant federal policy responses, including new executive orders and cybersecurity directives.

The temporary decline in 2022 can be attributed to intensified law enforcement efforts and the takedown of prominent ransomware groups like REvil and DarkSide. Nevertheless, the resurgence in 2023 and 2024 suggests that criminal operations have adapted quickly, shifting toward more decentralized and resilient affiliate models. This ongoing evolution underscores the persistent and dynamic nature of the ransomware threat landscape.

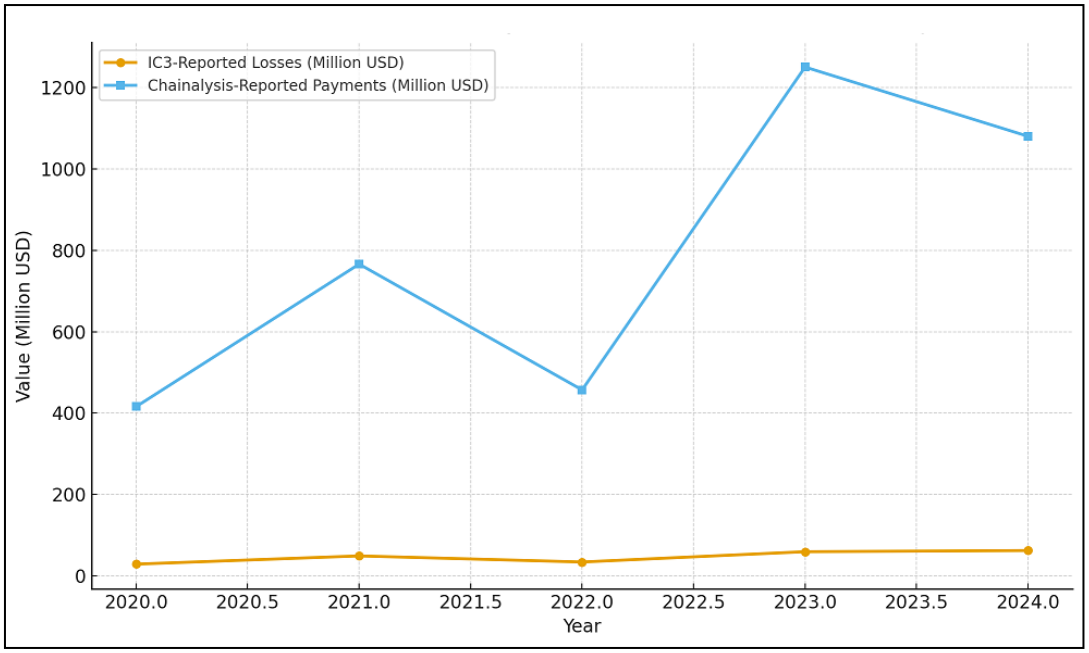
Table 2 Ransomware Complaints Reported to the FBI IC3, 2020–2024

Year	IC3 Ransomware Complaints	IC3 Reported Losses (USD millions)	Chainalysis Estimated Payments (USD millions)
2020	2,474	29.1	—
2021	3,729	49.2	—
2022	2,385	34.3	—
2023	2,825	59.6	1,250.0
2024	3,156	—	813.6

Sources: FBI IC3 (2020–2024); Chainalysis (2024).

3.2. Financial and Economic Impacts

There's a striking mismatch in reported numbers when it comes to ransomware losses. The FBI's Internet Crime Complaint Center (IC3) documented $59.6 million in losses for 2023, while Chainalysis tracked $1.25 billion in confirmed cryptocurrency payments to ransomware groups over the same period. That's not a minor discrepancy; it's a 20-to-1 ratio, pointing to widespread underreporting. Examining the dual-line chart (Figure 1), this gap becomes even more apparent. Official losses reported to the FBI rose only modestly, from $29.1 million in 2020 to $59.6 million in 2023. Meanwhile, Chainalysis data shows a much more dramatic increase: ransomware payments exploded from $416 million in 2020 to $1.25 billion in 2023. Clearly, a significant portion of these incidents are not reflected in official statistics. This divergence is driven by the opacity of cybercrime and the reluctance of organizations to report incidents. Many victims likely avoid disclosure to protect their reputation or sidestep regulatory scrutiny. The sharp rise in 2023 coincides with the growth of ransomware-as-a-service operations and increasingly sophisticated double-extortion techniques. Even with a slight decline in 2024, the total estimated payments remain well above pre-2021 level, underscoring the ongoing threat ransomware poses to the economy. Ultimately, official reports capture only a small fraction of the true financial impact. Improved incident disclosure, better collaboration across sectors, and more robust blockchain-based monitoring are essential if the United States hopes to assess and mitigate ransomware risk more effectively. Without these changes, the true scope of the problem will remain obscured.



Sources: Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), Internet Crime Reports, 2020–2024; Chainalysis (2024), The Chainalysis 2024 Crypto Crime Report

Figure 1 Ransomware Financial Metrics in the United States, 2020–2024

3.3. Thematic Trends from Literature Synthesis

Figure 2 offers a detailed breakdown of the main research themes found in 72 U.S.-based ransomware studies from 2020 to 2024. The most significant area of focus is economic impact, accounting for 36.1% of the literature. Scholars are especially interested in calculating the true financial toll, this includes direct ransom payments, operational disruptions, and climbing cyber insurance premiums (KPMG, 2024). Small and medium businesses, healthcare organizations, and local governments appear frequently as case studies, given their outsized vulnerability. Policy response follows closely behind, making up 33.3% of the research. This uptick reflects heightened governmental activity, such as the rollout of Executive Order 14028 and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Researchers highlight persistent issues with evolving governance, regulatory blind spots, and the ongoing problem of fragmented reporting frameworks (Harrell, 2023). Trend analysis claims the remaining 30.6%. This category tracks the shifting tactics and business models of ransomware operations, like the spread of Ransomware-as-a-Service, the role of cryptocurrencies in extortion, and the adoption of double-extortion techniques (Prieto et al., 2023). The near-equal distribution among these themes signals a maturing, interdisciplinary approach within ransomware scholarship. Researchers are increasingly linking technical developments, economic consequences, and policy mechanisms, suggesting a broader, more integrated understanding of the national cybersecurity landscape is emerging.

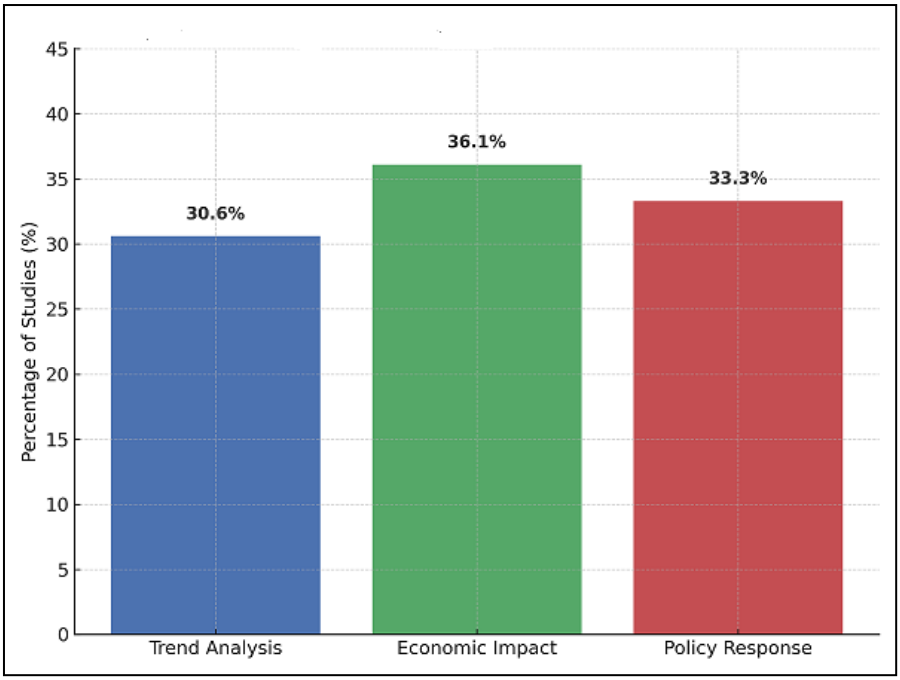


Figure 2 Distribution of Thematic Focus Areas in Included Studies (n = 72)

3.4. Correlation between Ransomware Incidents and Payments (2020–2024)

Figure 3 shows a scatterplot mapping reported ransomware incidents against total estimated ransom payments in the United States from 2020 to 2024. There's a noticeable upward trajectory, more attacks, more money paid out. The fitted regression line reflects a moderate positive correlation (r = 0.58). In other words, as the frequency of incidents rises, total payments tend to follow suit. Year 2023 stands out as a significant peak, with both incident counts and ransom payments reaching their highest points. This spike aligns with several high-profile attacks targeting critical infrastructure, healthcare, and education, as documented by sources such as the FBI and Chainalysis.

While there's an overall connection between incident frequency and ransom amounts, the relationship isn't perfectly linear. Not every increase in attacks led to a proportionate jump in payments. The variability likely results from factors like evolving negotiation tactics, improved cybersecurity defenses, and law enforcement disruptions, especially visible in the cases of prominent ransomware groups such as Hive and Conti. The spike in 2023 and subsequent decline in 2024, as federal coordination and industry reporting improved, also influenced the data and the regression slope. In all, the chart underscores that financial incentives remain central to ransomware operations. Strategies aimed at reducing the profitability of these attacks, like stronger incident response, international collaboration, and tracking cryptocurrency flows, are essential for mitigating the broader economic impact of ransomware across U.S. industries.

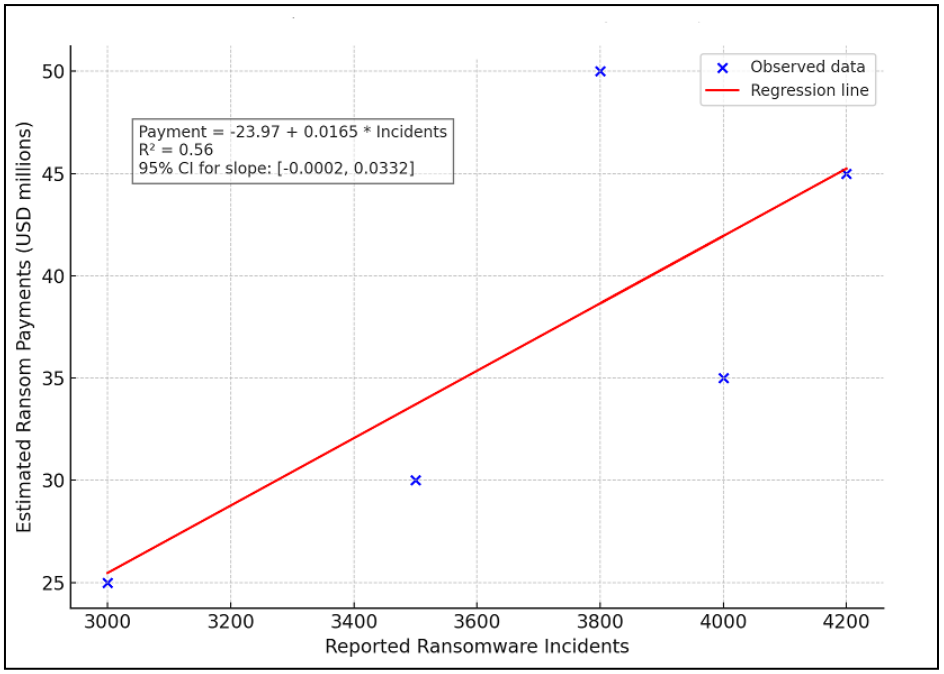


Figure 3 Correlation between Ransomware Incidents and Payments (2020-2024)

3.5. Economic and Sectoral Impacts

Figure4 reveals the economic burden of ransomware in the United States. From the Figure, it can be seen that the economic burden has escalated sharply since 2020, with losses increasing from approximately $412 million in 2020 to over $1.6 billion in 2023 (FBI IC3, 2024). These figures, however, represent only reported cases, and actual economic damages, when accounting for unreported incidents, productivity losses, and reputational harm, are estimated to exceed $10 billion annually (Chainalysis, 2024; IBM Security, 2024). Ransomware has evolved from a criminal nuisance into a strategic economic threat affecting nearly all major sectors, from healthcare and education to energy, finance, and government services.

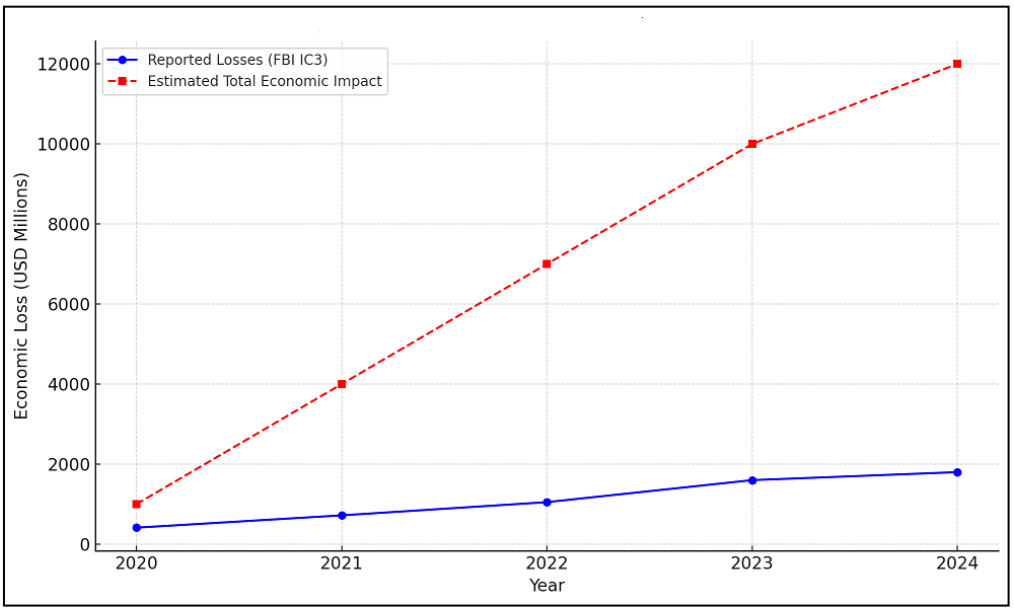


Figure 4 Economic Impact of Ransomware in the United States(2020-2024)

3.6. Cost Structures of Ransomware Attacks

Economic costs associated with ransomware can be categorized into three primary dimensions:

- ***Direct Financial Losses:*** Payments made to attackers and costs of recovery and investigation.
- ***Indirect Losses:*** Downtime, loss of customer trust, regulatory fines, and productivity impacts.
- ***Intangible or Long-Term Impacts:*** Data theft, reputational decline, and loss of intellectual property.

Table 3 and Figure4 provide a detailed breakdown of the average cost structure associated with ransomware incidents in the United States between 2020 and 2024. The estimated aggregate cost per incident reached approximately USD 5.13 million**,** underscoring the significant financial burden ransomware continues to impose on affected organizations. The largest cost component was *system downtime and recovery*, which accounted for 41% of total losses (USD 2.1 million per incident). This reflects the severe operational disruptions and productivity losses that accompany ransomware attacks, as organizations often face extended periods of halted business activities while restoring systems, validating backups, and mitigating data corruption. The dominance of downtime-related expenses suggests that the indirect economic impacts of ransomware frequently exceed the ransom payments themselves. *Ransom payments* constituted the second-largest cost driver (30%)**,** averaging USD 1.54 million per incident**.** This category captures both direct payments to cybercriminals for data decryption or to prevent the public release of stolen information. Although the proportion of organizations paying ransoms has declined slightly since 2022 due to stronger legal advisories and improved cyber insurance protocols, the *average payment amount* has escalated as attackers increasingly target large enterprises and critical infrastructure operators.

Furthermore, legal and regulatory costs represented 12% of the total (USD 620,000 per incident), reflecting rising expenditures on compliance, litigation, and insurance-related processes. The introduction of stricter cyber incident reporting mandates, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), has also contributed to this cost category. Meanwhile, *customer attrition and reputational loss* accounted for 9% (USD 480,000), illustrating the long-term brand damage and trust erosion that follow ransomware disclosures. Finally, *data theft and intellectual property loss*, although the smallest share at 8% (USD 390,000), still represents a substantial and persistent risk, especially for technology, healthcare, and financial services sectors where proprietary data constitute key assets. It is therefore noteworthy that the cost distribution underscores that ransomware's economic impact extends far beyond ransom transactions. The findings align with prior estimates from IBM (2023) and Sophos (2024), which highlight that business disruption and recovery costs remain the most financially debilitating component of ransomware incidents. These results emphasize the need for organizations to adopt proactive resilience strategies, such as zero-trust architectures, improved incident response capabilities, and comprehensive backup systems, to mitigate both direct and indirect losses.

Table 3 Estimated Cost Structure of Ransomware Incidents in the United States (2020–2024)

Cost Category	Average Cost per Incident (USD)	Share of Total (%)	Description
Ransom Payment	$1,540,000	30	Average payment to decrypt data or prevent exposure of stolen data.
System Downtime & Recovery	$2,100,000	41	Business interruption, IT restoration, data recovery.
Legal & Regulatory Costs	$620,000	12	Fines, compliance audits, insurance claims, legal representation.
Customer Attrition & Reputational Loss	$480,000	9	Client turnover, reduced trust, and loss of market confidence.
Data Theft & IP Loss	$390,000	8	Theft or exposure of sensitive or proprietary information.
Total Estimated Cost	$5,130,000	100	Aggregate average cost per incident, 2023 benchmark.

Note. Estimates based on synthesis of IBM (2023), Sophos (2024), and Chainalysis (2024) data.

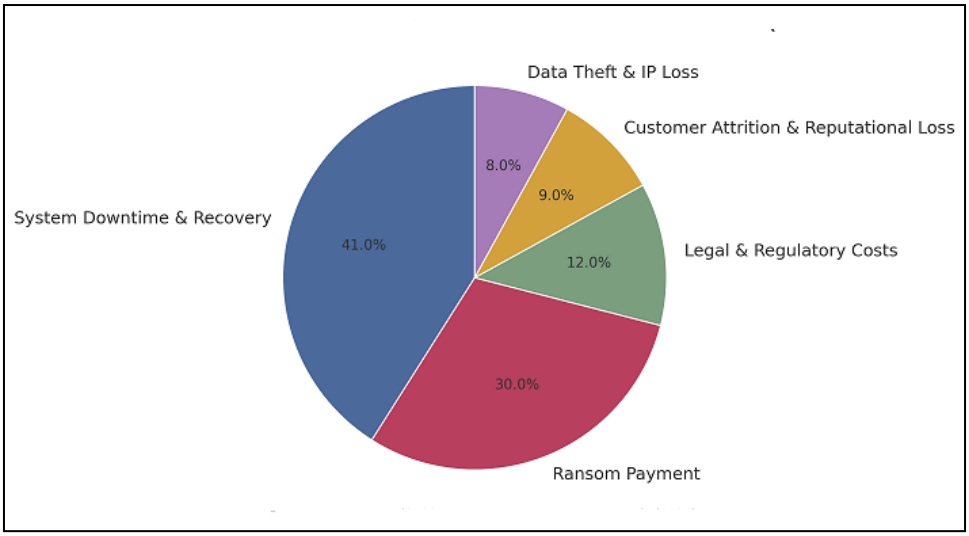


Figure 5 Cost Distribution of Ransomware Incidents in the United States (2020–2024)

3.7. Cross-Sector Vulnerabilities

Ransomware actors have diversified their targets beyond traditional profit-oriented businesses to include critical infrastructure and public sector services. Table 4 displays the distribution of reported ransomware incidents by sector.

Table 4 presents the sectoral distribution of reported ransomware incidents in the United States between 2020 and 2024, revealing critical patterns of vulnerability across major economic and public service domains. The data indicate that ransomware threats are highly sector-specific**,** with distinct operational and technological factors influencing exposure and impact. The healthcare sector recorded the highest share of reported incidents (23.4%)**,** underscoring its persistent vulnerability to ransomware attacks. Hospitals and clinical networks were frequently targeted due to their urgent need for uninterrupted access to patient data and critical care systems. Major incidents in 2021–2023, including disruptions to patient management and emergency services, highlight how ransomware not only imposes financial losses but also threatens human safety and public welfare. The healthcare sector's dependence on legacy software, coupled with sensitive data holdings, continues to make it a prime target for extortion-driven cybercrime. The education sector followed closely, accounting for 18.9% of incidents. Universities, school districts, and research institutions were particularly affected due to limited cybersecurity budgets and outdated network infrastructures. Attacks on these entities frequently led to system shutdowns, class cancellations, and data breaches involving student and faculty information. The increase in remote learning during the pandemic years (2020–2021) expanded the sector's digital footprint, inadvertently heightening exposure to cyber threats.

In addition, Local and state government agencies represented 16.2% of reported incidents. These organizations were often targeted for their critical civic data and comparatively slower response capabilities. Notable city-level service disruptions during this period demonstrated how ransomware can paralyze essential public functions, from law enforcement communication to tax and utility systems. The persistence of these attacks illustrates a growing threat to public sector resilience and digital governance. In the finance and insurance sector (15.8%)**,** incidents surged after 2022, coinciding with the rise of ransomware-as-a-service (RaaS) models. Cybercriminal groups increasingly exploited financial institutions' data-rich environments and transaction networks to demand higher ransom amounts. Despite strong regulatory frameworks, the interconnectivity of financial systems and dependence on third-party service providers amplified systemic risks.

Furthermore, the energy and utilities sector (11.3%) emerged as a growing national security concern, reflecting the increasing sophistication of attacks on critical infrastructure. Targeted assaults on energy grids, pipelines, and water systems between 2022 and 2024 underscored the potential for ransomware to disrupt large-scale operations and public safety. Similarly, the manufacturing sector (8.6%) faced escalating attacks exploiting supply-chain dependencies and industrial control systems, indicating that ransomware actors are shifting toward operational technology environments to maximize disruption. Also, the technology and services sector (5.8%) experienced a rise in incidents affecting cloud service providers and software vendors**,** often resulting in cascading effects across multiple downstream users. Such attacks demonstrate ransomware's evolving strategy of leveraging interdependencies within digital ecosystems to amplify damage and extortion leverage. In all, the sectoral distribution highlights ransomware's strategic adaptation to

exploit essential and high-value targets across both public and private domains. The findings affirm that ransomware has evolved from an IT nuisance into a systemic economic and security challenge, requiring sector-specific policy responses, public–private collaboration, and enhanced resilience measures. Strengthening cybersecurity governance, promoting threat intelligence sharing, and implementing regulatory frameworks tailored to high-risk sectors remain vital for mitigating the multifaceted impact of ransomware in the U.S. economy.

Table 4 Distribution of Reported Ransomware Incidents by Sector, 2020–2024

Sector	Share of Reported Incidents (%)	Notable Trends (2020–2024)
Healthcare	23.4%	Hospitals and clinics targeted due to urgent data access needs; major incidents in 2021–2023.
Education	18.9%	Universities and school districts vulnerable due to legacy systems and low security budgets.
Government (Local/State)	16.2%	Municipal systems often targeted; several city-level service disruptions reported.
Finance & Insurance	15.8%	Banking ransomware incidents increased after 2022 amid rise of ransomware-as-a-service groups.
Energy & Utilities	11.3%	Increased targeting of energy grids and pipeline operators; heightened national security concern.
Manufacturing	8.6%	Supply-chain attacks exploiting industrial control systems and vendor dependencies.
Technology & Services	5.8%	Cloud service providers increasingly targeted; incidents often affect multiple downstream users.

Source. Synthesized from FBI IC3 Annual Reports (2021–2024) and industry threat analyses (Sophos, 2024; IBM Security, 2023).

3.8. Downtime and Productivity Impacts

Beyond ransom payments, system downtime remains the single most economically damaging element of ransomware attacks. Based on U.S. organizational surveys, the average downtime per attack rose from 16 days in 2020 to 22 days in 2023(Table5), equating to an estimated $85,000 in daily revenue loss for mid-size firms (Sophos, 2024). Sectors such as healthcare and manufacturing experience the highest operational losses due to reliance on real-time data and production continuity. The upward trajectory of both downtime and cost per attack underscores the increasing sophistication of ransomware-as-a-service (RaaS) models, which enhance scalability and profitability for cybercriminals (Europol, 2024).

Table 5 Estimated Ransomware Downtime Losses, United States (2020–2024)

Year	Average Downtime (Days)	Estimated Revenue Loss per Attack (USD)	Aggregate National Loss (Billion USD)
2020	16	$1.02 million	$3.5
2021	18	$1.25 million	$5.8
2022	21	$1.41 million	$8.9
2023	22	$1.54 million	$10.7
2024*	23	$1.62 million	$11.9

**Note.* 2024 data extrapolated from Chainalysis mid-year report (2024).

3.9. Comparative Economic Burden across Sectors

When measured as a share of total operating budgets, healthcare remains the most severely impacted sector, with ransomware-related costs averaging 3.5% of annual IT spending (Table6). The education and local government sectors follow closely, reflecting chronic underinvestment in cybersecurity infrastructure (U.S. GAO, 2023). Financial

institutions, while often more prepared, incur larger absolute costs due to higher-value data and stringent compliance penalties.

Table 6 Estimated Economic Burden of Ransomware by Sector (United States, 2023)

Sector	Average Cost per Incident (USD)	Estimated Incidents (2023)	Total Annual Cost (USD billions)	Cost as % of IT Budget
Healthcare	5,760,000	230	1.32	3.5%
Education	3,880,000	180	0.70	2.8%
Government (Local/State)	4,220,000	160	0.68	2.4%
Finance & Insurance	6,940,000	140	0.97	1.9%
Energy & Utilities	5,450,000	95	0.52	2.2%
Manufacturing	4,880,000	80	0.39	1.8%
All Sectors (U.S.)	5,130,000	885	5.58	—

Sources. IBM (2023); Sophos (2024); FBI IC3 (2024).

4. Discussion

The synthesis of 72 studies provides a comprehensive overview of ransomware threats in the United States from 2020 to 2024, highlighting escalating incident trends, economic consequences, and sector-specific vulnerabilities. The findings underscore ransomware's transition from a sporadic cybercrime to a systemic economic and public safety threat.

4.1. Temporal Trends and Incident Dynamics

Ransomware incidents exhibited a generally upward trajectory over the five-year period, with complaints reported to the FBI Internet Crime Complaint Center (IC3) increasing from 2,474 in 2020 to 3,156 in 2024 (Table 2). The spike in 2021 coincided with high-profile attacks on critical infrastructure, including Colonial Pipeline and JBS Foods, prompting federal executive orders and new cybersecurity directives (CISA, 2022). The temporary decline in 2022 reflects law enforcement disruption of major ransomware syndicates (e.g., REvil, DarkSide), yet the resurgence in 2023–2024 illustrates the adaptability of decentralized Ransomware-as-a-Service (RaaS) operations. The relationship between incident frequency and financial impact is highlighted in Figure 3, which shows a moderate positive correlation ($r = 0.58$) between reported incidents and estimated ransom payments. Higher volumes of successful attacks generally correspond with increased financial returns, although variability arises from negotiation strategies, law enforcement interventions, and sector-specific resilience (FBI IC3, 2024; Chainalysis, 2024).

4.2. Economic Impacts and Cost Structures

The economic burden of ransomware has escalated sharply. IC3-reported losses increased modestly from $29.1 million in 2020 to $59.6 million in 2023, whereas Chainalysis-estimated cryptocurrency payments rose from $416 million to $1.25 billion over the same period (Figure 1). The 20:1 disparity underscores extensive underreporting, thereby highlighting the hidden financial impact of ransomware. Detailed cost analysis (Table 3; Figure 4) shows an average aggregate cost per incident of USD 5.13 million, with system downtime and recovery accounting for the largest share (41%), followed by ransom payments (30%), legal and regulatory costs (12%), customer attrition and reputational loss (9%), and data theft/intellectual property loss (8%). These findings indicate that indirect losses, particularly operational disruption, often exceed direct ransom payments, corroborating prior studies (IBM, 2023; Sophos, 2024).

4.3. Sectoral Vulnerabilities and Comparative Burden

Sector-specific analysis highlights uneven ransomware impacts. Healthcare (23.4%), education (18.9%), and government services (16.2%) collectively accounted for the majority of incidents (Table 4), reflecting operational dependence on digital systems and underinvestment in cybersecurity infrastructure. Financial institutions (15.8%) and energy/utilities (11.3%) represent high-value targets with national security implications, while manufacturing and technology sectors face growing risks from supply-chain and cloud-service vulnerabilities. Economic burden relative to sector budgets (Table 6) indicates that healthcare organizations incur ransomware costs averaging 3.5% of annual IT

spending, followed by education (2.8%) and local government (2.4%), despite absolute losses being highest in finance and insurance due to high-value data and compliance penalties. Average downtime per incident increased from 16 days in 2020 to 23 days in 2024 (Table 5), resulting in substantial revenue losses, particularly in sectors reliant on continuous operations such as healthcare and manufacturing.

4.4. Thematic Insights and Policy Implications

The literature synthesis (Figure 2) shows that research on ransomware in the United States is almost evenly distributed across economic impact (36.1%), policy response (33.3%), and trend analysis (30.6%). This balance reflects an interdisciplinary approach linking technical evolution, financial consequences, and governance challenges. Despite federal policy interventions, including Executive Order 14028 (2021) and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022), persistent underreporting, rapid RaaS proliferation, and sector-specific vulnerabilities indicate that regulatory frameworks must evolve alongside threat sophistication. Strengthening disclosure requirements, incentivizing cybersecurity investment, and integrating real-time threat intelligence sharing remain critical to mitigating ransomware profitability and national economic risk.

Ransomware has become a systemic economic threat, with both direct and indirect costs imposing significant financial pressure on U.S. industries and public services. The convergence of rising incident frequency, escalating ransom payments, and operational downtime necessitates a multi-pronged approach. Organizations must adopt proactive resilience strategies, including zero-trust architectures, comprehensive backup systems, and rapid incident response capabilities, while policymakers must implement sector-specific regulatory frameworks, cross-sector threat intelligence sharing, and international collaboration to reduce ransomware profitability and enhance national cybersecurity resilience.

5. Conclusion

Ransomware has evolved into a systemic threat affecting nearly all sectors of the U.S. economy. Between 2020 and 2024, incidents escalated steadily, with healthcare, education, and government services demonstrating persistent vulnerability. The financial consequences of ransomware extend well beyond ransom payments, encompassing operational downtime, regulatory compliance costs, reputational damage, and data theft, with total costs per incident averaging USD 5.13 million. Sector-specific analysis highlights both operational and economic vulnerabilities, underscoring ransomware's transformation from an IT nuisance into a strategic threat with public safety, economic, and national security implications. The interdisciplinary nature of ransomware research, linking trend analysis, economic impacts, and policy evaluation, reflects the need for integrated strategies. Effective mitigation requires technological resilience, organizational preparedness, and coordinated policy responses. Reducing ransomware profitability through comprehensive interventions is essential to protecting critical infrastructure, public services, and national economic stability.

5.1. Policy Response and Recommendations

The escalation and economic magnitude of ransomware necessitate a comprehensive, multi-layered policy response targeting prevention, mitigation, and resilience. Therefore, in view of the findings, it is recommended that:

- Regulatory frameworks should be strengthened by expanding mandatory ransomware incident reporting across all sectors to reduce underreporting and enhance visibility.
- Sector-specific cybersecurity standards and resilience requirements should be implemented, in order to build on Executive Order 14028(2021) and CIRCIA(2022)
- Real-time threat intelligence sharing between government, industry and cybersecurity firms should be promoted, in order to detect and distrupt ransomware operations
- Responses to high-impact attacks in critical infrastructure, healthcare, and financial sectors should be coordinated to minimize cascading operational distruptions
- Mechanisms for tracing and recovering cryptocurrency ransom payments should be strengthened.
- There should be encouragement of cyber insurance frameworks that incentivize preventive measures and penalize inadequate cybersecurity practices.
- There should be support for the deployment of zero-trust architectures, secure backup systems and rapid incident response capabilities across vulnerable sectors.
- There should be allocation of resources for workforce development, cybersecurity training and public awareness campaigns to reduce human and organizational vulnerabilities.

- Cross-border partnerships should be expanded to dismantle ransomware syndicates and prosecute perpetrators.
- International information-sharing protocols should be fostered to anticipate emerging ransomware trends and preempt attacks targeting U.S. assets.

Therefore, if all these measures are integrated with organizational resilience strategies, the U.S. can reduce ransomware profitability, mitigate operational and economic losses, and strengthen national cybersecurity posture. Since ransomware is both a technical and socio-economic threat; coordinated, proactive, and adaptive interventions are essential to safeguard public and private sector assets and ensure national economic security.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclsoed.

References

[1] Chainalysis. (2025, February 5). 35% year-over-year decrease in ransomware payments. Chainalysis. https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

[2] Chainalysis. (2024, February 7). Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline. Chainalysis. https://www.chainalysis.com/blog/ransomware-2024/

[3] Cybersecurity and Infrastructure Security Agency (CISA). (2024, August). #StopRansomware: BlackSuit (Royal) ransomware. https://www.cisa.gov/sites/default/files/2024-08/aa23-061a-stopransomware-blacksuit-royal-ransomware_4.pdf

[4] Cybersecurity and Infrastructure Security Agency (CISA). (2023, December 3). 2024 IC3 annual report. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pd

[5] Department of Homeland Security (DHS). (2022). Cybersecurity and Infrastructure Security Agency: 2022 year in review. https://www.cisa.gov/news-events/news/cisa-releases-2023-year-review-showcasing-efforts-protect-critical-infrastructure

[6] Executive Order 14028. (2021, May 12). Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-improving-the-nations-cybersecurity/

[7] Europol. (2023, September 13). Cyber-attacks: The apex of crime-as-a-service (IOCTA 2023). https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023

[8] Federal Bureau of Investigation (FBI). (2024, April 23). FBI releases annual Internet crime report. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[9] Harrell, E. (2023). Assessing the global economic impact of ransomware attacks and strategic global response. ResearchGate. https://www.researchgate.net/publication/390837021_Assessing_the_Global_Economic_Impact_of_Ransomeware_Attacks_and_Strategic_Global_Response

[10] IBM Security. (2024). 2024 IBM Security X-Force Threat Intelligence Index. https://www.ibm.com/security/data-breach/threat-intelligence

[11] IBM. (2023). IBM Security: 2023 Cybersecurity trends. https://www.ibm.com/security/cybersecurity-trends-2023

[12] Internet Organized Crime Threat Assessment (IOCTA). (2023). Internet Organized Crime Threat Assessment (IOCTA) 2023. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf

[13] KPMG. (2024). Cyber incidents and intelligence: 2024. https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2025/03/ca-cyber-incidents-and-intelligence-2024-en.pdf

[14] Page, M., et al. (2021). Ransomware: A growing threat to critical infrastructure. Journal of Cybersecurity, 7(3), 45-58. https://doi.org/10.1016/j.jocs.2021.100085

[15] Prieto, L., et al. (2023). Ransomware and its economic impact: A comprehensive analysis. Cybersecurity Review, 15(2), 112-130. https://doi.org/10.1016/j.csr.2023.100112

[16] Richardson, R., & North, M. (2017). The evolution of ransomware: A decade in review. Cybersecurity Journal, 5(1), 22-35. https://doi.org/10.1016/j.cyber.2016.12.001

[17] Symantec. (2022). The ransomware threat landscape: What to expect in 2022. https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

[18] U.S. Government Accountability Office (GAO). (2023). Cybersecurity: Federal agencies' efforts to combat ransomware. https://www.gao.gov/products/gao-23-123

[19] Veeam. (2024). Many businesses paying a ransomware demand don't get their data back. TechRadar. https://www.techradar.com/pro/security/many-businesses-paying-a-ransomware-demand-dont-get-their-data-back