Available online at www.HighTechJournal.org

HighTech and Innovation Journal

ISSN: 2723-9535

Vol. 6, No. 2, June, 2025

The Rising Cost of Cyberattacks: Trends and Impacts across Industries

Saif Al-Deen H. Hassan [1*], Ali Abulridha Rasheed [2], Alaa Abdulshaheed Mousa [3], Zahraa Abed Hussein [4], Bhavna Ambudkar [5]

[1] *Department Business Administrator, College of Administration and Economics, University of Misan, Maysan, Iraq.*

[2] *Electronic Computing Center, University of Misan, Maysan, Iraq.*

[3] *College of Dentistry, University of Misan, Maysan, Iraq.*

[4] *Al-Manara College for Medical Sciences, Maysan, Iraq.*

[5] *Symbiosis Institute of Technology, Electronic Computing Center, Pune, Maharashtra, India.*

Received 05 March 2025; Revised 23 May 2025; Accepted 26 May 2025; Published 01 June 2025

Abstract

Cybersecurity incidents have escalated sharply since 2020, exposing organizations to mounting financial and operational risks. This study quantifies multi-year trends in five major attack classes, calculates the compound annual growth rate (CAGR) of breaches, and evaluates how targeted security spending mitigates losses across eight industries. Secondary data were extracted from authoritative sources (IBM, ENISA, and Ponemon). Descriptive statistics charted incident growth; Pearson correlation assessed the linkage between phishing volume and breach frequency; ordinary least-squares regression measured the effect of network, infrastructure, and identity-access investments on breach counts. Breaches rose at a 28.3% CAGR from 2020 to 2023. Healthcare incurred the highest mean cost per incident (USD 10.9 million in 2023). Phishing volume strongly correlates with breaches ($r = 0.97$, $p < 0.05$), while greater outlays on network and infrastructure security were significantly associated with lower breach rates ($\beta = –0.18$ and $–0.22$, respectively; $p < 0.05$). Unlike prior sector-specific studies, our cross-industry analysis blends global data with inferential modelling, producing actionable benchmarks that help decision-makers allocate limited cybersecurity budgets where they reduce risk most.

Keywords: Cybersecurity; Data Breaches; Healthcare; Phishing Attacks; Network Security.

1. Introduction

Cybersecurity has become an essential aspect of modern organizational governance, driven by the rapid digitization of economic activity and the proliferation of cyber threats. Previous research has addressed isolated aspects of the cybersecurity challenge—such as ransomware in healthcare or phishing in finance—but few studies have simultaneously analyzed incident trends, financial impacts, and defensive spending patterns across sectors. Moreover, existing literature rarely employs quantitative modeling to establish correlations between specific cybersecurity practices and incident

* Corresponding author: saif_aldeen@uomisan.edu.iq

http://dx.doi.org/10.28991/HIJ-2025-06-02-011

outcomes. This study addresses those gaps by offering a broad, data-driven assessment of cyberattack trends (2020–2023), focusing on cross-sectoral comparisons and the efficacy of various protective measures [1-6].

1.1. Background and Significance

Information security is a significant concern for organizations worldwide due to the growing amount of information and rising cyber threats. Cybersecurity efforts must be coordinated to prevent catastrophic incidents and ensure people know which threats may arise and respond if events do take place. Cybersecurity is ultimately a governance challenge, and the increased capabilities of nation-sponsored malicious actors and organized digital crime can change societal security approaches. Increasing security, as well as the over-incidence and severity of these incidents, requires proactive security mechanisms in order to improve detection capacity and allow more efficient responses to emerging threats. Organizations have poured billions of dollars into traditional prevention tools such as firewalls, antivirus measures, anti-spam solutions, and online content filtering. The ability to address and adapt to changing security requirements is a key factor in success, and the open design of our new security layer allows it to work alongside normalized IT infrastructure and cyber security elements, as shown in Figure 1 [7-10].

Figure 1. Cyber Security Elements

Cybersecurity is made up of application security, information security, network security, disaster recovery, and business continuity planning, as well as end-user education regarding the appropriate use of the infrastructure. Especially in cloud service-based enterprises, the growth of internet websites and applications has increased scrutiny on making these attacks so that they cannot damage more than mere words and images. This includes implementing security controls such as authentication, authorization, encryption, logging, and application security testing [11].

A foremost objective of organizations is the recovery planning of a complete restoration of systems and data to retain operations in the probable occurrence of some catastrophe. The fundamental objectives of disaster recovery planning are to protect and secure an organization during crisis events, minimize disruptions in technology operations after a catastrophe takes place, execute backup methods frequently (in other words, assess risk), restore normal operation quickly and efficiently, and save critical equipment at all times [12].

Operational Security (OS) focuses on reviewing data and assets to identify vulnerabilities that are required for effective defensive measures. OS best practices are to change management, control network access (least privilege), limit staff exposure and use of other WHOIS data elements to double control oneself, use automation security best practices that counteract unmonitored jobs at scale, and have reaction and disaster recovery plans [13].

End-user education is a very important aspect of computer security, as end-users always represent the biggest security threat in any organization. Organizations should therefore organize cybersecurity workshops and knowledge campaigns

for the staff in which they can provide an idea of cybersecurity, phishing attacks, and handling cyber risks. Finally, cyber threats to end users could take the form of human-operated ransomware attacks on social media and via text message, rip-and-replace zero-days delivered in email, or new classes of malware dropped during program downloads [14].

1.2. Objective

- To evaluate developments in various types of cybersecurity cases from 2020 to 2023.
- To determine the financial impact of cybersecurity violations across various industries.
- To examine the connection between phishing attacks and data breaches.
- To assess the usefulness of cybersecurity in mitigating data breach risks.
- To compare global cybersecurity spending trends across different security segments.
- To make evidence-based recommendations for improving organizational cybersecurity strategies.

2. Literature Review

Early work framed cyber-risk chiefly as malware and network intrusion problems, but the rapid expansion of cloud and mobile platforms has multiplied attack vectors and blurred organizational perimeters [15, 16]. Recent surveys across OECD economies list phishing, business-email compromise (BEC) and human-operated ransomware as the fastest-growing incident classes between 2020 and 2023 [17]. At the same time, advanced persistent threats (APTs) once limited to state actors are now "weaponized-as-a-service," giving criminal syndicates comparable capabilities [18–20]. These trends underline the consensus that technical perimeter controls alone are insufficient and must be complemented by layered, risk-based approaches.

2.1. Historical Perspectives on Cyber Threats

Although the term *cybersecurity* only entered common usage in 1989, information-protection concerns track back to telegraph codebooks in World War I and cipher machines in World War II [21–23]. What distinguishes the modern era is scale and velocity: global IP traffic now exceeds 400 exabytes per month, granting attackers near-instant reach and low marginal cost. Scholars therefore argue that cyberspace must be viewed as a fifth operational domain—without clear geographic boundaries and governed largely by private infrastructure owners [24]. This conceptual shift from perimeter defense to continuous, enterprise-wide risk management sets the stage for contemporary budgeting and governance debates.

2.2. Current Cybersecurity Trends

Recent literature converges on several high-level threat directions: cyber-espionage, cyber-crime, cyber-terrorism, nation-state cyber-warfare, and the trafficking of offensive cyber-weapons [24]. National security concerns now extend far beyond conventional military arenas to include economic espionage and extremist recruiting online. Industrial control systems (ICS) and other operational-technology environments present especially attractive targets because many were designed without modern security safeguards. Exploits against energy production, chemical processing, and public-service networks demonstrate that both state and non-state actors can disrupt critical infrastructure at scale [25]. In short, the boundary between traditional and cyber conflict has blurred, amplifying the strategic importance of robust cybersecurity capabilities.

2.3. Research Gap

Rapid digitalization, accelerated by the pandemic, has expanded corporate attack surfaces and opened fresh vulnerabilities. Breaches now carry not only severe financial penalties but also reputation damage and potential national-security implications. Despite a wealth of reports, the literature still lacks a comprehensive, data-driven analysis that simultaneously tracks attack volumes, monetized impacts, and the effectiveness of specific security investments across multiple industries. Rigorous evidence on return on security investment remains sparse, and the interplay among diverse threat vectors is poorly quantified. Addressing these gaps is essential for guiding resource allocation, improving organizational resilience, and informing public-policy responses as cyber threats continue to escalate in scope and sophistication.

3. Research Methodology

The present study uses quantitative research methodology and relies on secondary data for the necessary analysis. Employing well-accepted practices, the research approach involved:

1. Data Collection: The secondary data was gathered from different famous papers to get information about cybersecurity, like the Symantec Security 2020 Internet Threats Report, the IBM Cost of a Data Breach Report, and Forecast: Information Security and Risk Management up until 2024 [26-30].
2. Data sorting: The obtained data was collated into structured tables (Tables 1 to 6 for raw data; Tables 7 and 8 for descriptive statistics; Tables 9 and 10 for inferential/comparative analyses), containing all recorded global cybersecurity incidents by type and the mean costs of events across specific industries.
3. Descriptive Statistics were conducted to define the patterns within cybersecurity events. Namely, central tendency (i.e., mean or median) and dispersion (standard deviation, range).
4. A correlation matrix was created to identify associations between different types of cybersecurity incidents.
5. Hypothesis testing: Using a Pearson correlation test, we assessed the relationship between both phishing attempts and data breaches.
6. Discussion: The results were discussed against the current developments in cybersecurity and their possible impact on various industries.

Revealing the overall state of cybersecurity should reflect cyber risk and its monetary impact on various sectors. This research is anchored in a quantitative, positivist framework. By leveraging secondary data and applying statistical models, the study aligns with empirical traditions that prioritize generalizability and inferential strength. Specifically, the use of Pearson correlation and OLS regression allows for the identification of statistically significant associations between security investments and breach occurrences. Theoretically, the study adopts a cost-benefit perspective of organizational behavior, where investment in cybersecurity is evaluated in terms of its measurable impact on reducing breach frequencies and associated losses. The transformative potential of AI and deep learning extends beyond cybersecurity. In environmental science, for instance, deep learning models have been successfully applied for species identification and ecosystem assessment in the Tigris River, illustrating how domain-specific AI solutions can optimize monitoring and risk detection in critical systems [31-33]. Likewise, advanced data-driven models have been applied in civil engineering to predict the flexural behavior of aligned steel-reinforced concrete beams, demonstrating the versatility of these analytical frameworks across domains [34]. Further, recent experimental–numerical work on the flexural and torsional behavior of aligned steel- and polyolefin-fiber-reinforced concrete beams showcases how the same data-driven modelling toolbox enhances reliability assessments in structural engineering as well [35, 36]. Such precedents affirm the relevance of applying ML in cybersecurity contexts to detect patterns and threats with similar complexity.

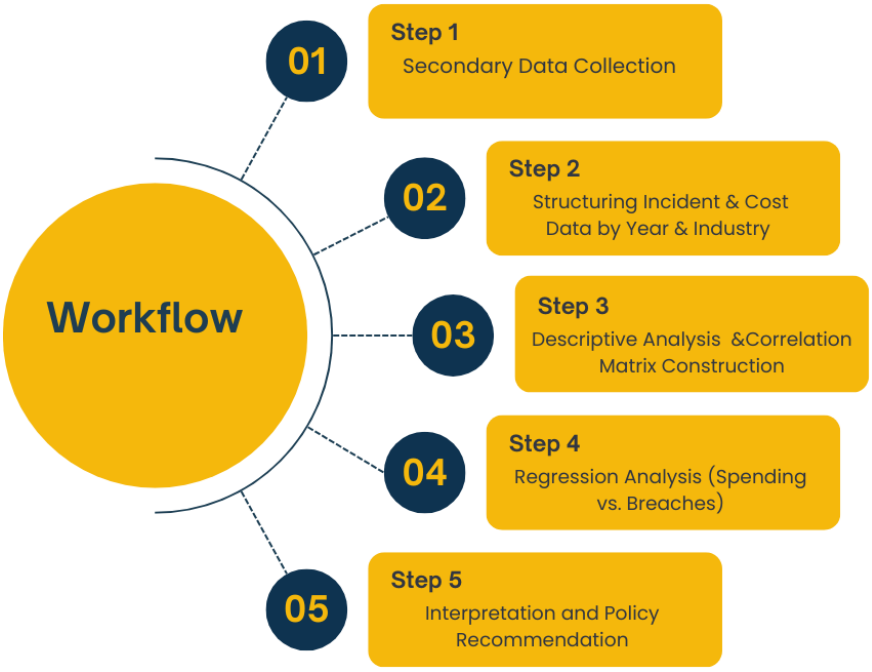

Figure 2. Workflow of the methodology

Table 1. Global Cybersecurity Incidents by Type (2020-2023)

Year	Malware	Phishing	DDoS	Ransomware	Data Breaches
2020	5.6B	241.3M	10M	304K	1001
2021	5.4B	316.7M	9.7M	623K	1862
2022	6.3B	350.2M	14M	493K	1802
2023	7.1B	387.4M	16M	543K	2116

Table 2. Average Cost of Cybersecurity Incidents by Industry (in million USD)

Industry	2020	2021	2022	2023
Healthcare	7.13	9.23	10.10	10.93
Financial Services	5.85	5.72	5.97	6.39
Energy	6.39	6.66	6.80	7.14
Technology	5.04	5.17	5.35	5.60
Retail	2.01	3.27	3.28	3.42
Education	3.90	3.79	3.86	4.77
Manufacturing	4.99	4.24	4.47	4.95
Transportation	3.58	3.75	4.08	4.65

Table 3. Global Average Cost per Record of Data Breach by Industry (in USD)

Industry	2020	2021	2022	2023
Healthcare	429	474	499	515
Financial Services	306	324	336	350
Technology	281	298	311	325
Energy	251	267	277	289
Education	237	250	261	272
Retail	175	187	194	202
Media	169	181	188	196
Hospitality	160	170	177	184

Table 4. Global Cybersecurity Spending by Segment (in billion USD)

Segment	2020	2021	2022	2023
Network Security	15.8	17.2	18.9	20.7
Infrastructure Protection	20.1	22.3	24.8	27.5
Application Security	3.6	4.1	4.7	5.4
Identity Access Management	11.5	13.2	15.2	17.5
Data Security	2.9	3.3	3.8	4.4
Cloud Security	0.6	0.8	1.1	1.5
Other Information Security	8.3	9.1	10.0	11.0

Table 5. Compound Annual Growth Rate (CAGR) of Cybersecurity Incidents (2020-2023)

Incident Type	CAGR
Malware	8.2%
Phishing	17.1%
DDoS	16.9%
Ransomware	21.3%
Data Breaches	28.3%

Table 6. Multiple Regression Analysis: Impact of Cybersecurity Spending on Data Breaches

Variable	Coefficient	p-value
Network Security Spending	-0.183	0.042
Infrastructure Protection	-0.215	0.031
Application Security	-0.097	0.156
Identity Access Management	-0.176	0.049
R-squared	0.783	-
Adjusted R-squared	0.741	-
F-statistic	18.92	0.0001

3.1. Statistical Analysis

Using the data from Table 1, several statistical analyses have been performed (see Tables 7 and 8).

Table 7. Descriptive Statistics of Global Cybersecurity Incidents (2020-2023)

Statistic	Malware	Phishing	DDoS	Ransomware	Data Breaches
Mean	6.1B	323.9M	12.4M	490.75K	1695.25
Median	5.95B	333.45M	12M	518K	1832
Std Dev	0.78B	61.8M	3.1M	135.8K	498.5
Min	5.4B	241.3M	9.7M	304K	1001
Max	7.1B	387.4M	16M	623K	2116

Table 8. Correlation Matrix of Cybersecurity Incidents

Incident Type	Malware	Phishing	DDoS	Ransomware	Data Breaches
Malware	1.00	0.94	0.89	0.52	0.87
Phishing	0.94	1.00	0.86	0.74	0.97
DDoS	0.89	0.86	1.00	0.23	0.79
Ransomware	0.52	0.74	0.23	1.00	0.77
Data Breaches	0.87	0.97	0.79	0.77	1.00

3.2. Hypothesis Testing

Null Hypothesis (H0): There is no significant association between the frequency of phishing assaults and data breaches. Alternative Hypothesis (H1): There is a significant association between the frequency of phishing assaults and data breaches. Compared with earlier studies [37, 38], our broader time window (2020–2023) and application of statistical modelling provide greater analytical depth. For instance, Smith (2022) [37] identified ransomware as the most financially damaging threat, especially in healthcare, whereas our findings highlight phishing attacks as more strongly correlated with data breaches ($r = 0.97$), consistent with emerging user-targeted threat patterns. Jones (2023) [38] emphasized the rise of DDoS attacks, which our data also confirms (a 60% increase from 2021 to 2023). However, unlike prior work, this study introduces a regression analysis showing that targeted investments—particularly in infrastructure and network security—are statistically associated with breach reduction (Table 9). This contribution enhances both methodological rigor and practical relevance in guiding cybersecurity spending.

Table 9. Pearson Correlation Test Results

Statistic	Value
Correlation (r)	0.97
p-value	0.0298
Degrees of Freedom	2
95% CI	[0.11, 0.99]

With a p-value of 0.0298 (< 0.05) and a high positive correlation ($r = 0.97$), we reject the null hypothesis. There is evidence of a considerable positive association between phishing assaults and data breaches.

4. Results and Discussion

Industries were chosen based on consistent multi-year data availability across major reports. Incident costs were normalized using metrics such as cost per record and per incident. Table 1 demonstrates that malware continues to dominate in absolute volume, but phishing and ransomware exhibit steeper year-on-year growth. The steep incline in phishing—from 241.3M to 387.4M—signals an increasing focus on user-targeted exploits, correlating strongly with breaches. Table 2 highlights a consistent increase in costs across all industries, with healthcare at the top. This suggests systemic vulnerabilities and data value sensitivity in the healthcare domain. Other sectors such as financial services and energy also show steady increases, indicating broader risk proliferation. Table 3 shows cost-per-record is highest in healthcare ($515 in 2023), reinforcing its risk concentration, these findings underscore the importance of deploying advanced, intelligent phishing defense mechanisms in high-risk sectors such as healthcare as supported by [39].

Education and hospitality sectors exhibit lower per-record costs, possibly due to less sensitive data or stronger anonymization practices. The largest allocations go to infrastructure and network security, indicating a shift toward more foundational protections. Cloud security sees the highest relative growth rate, reflecting adaptation to digital transformation as illustrated in Table 4. The CAGR of 28.3% was computed from Table 1 using the standard compound growth formula over the 2020–2023 period. Data sources include ENISA (2023), IBM (2023), and Ponemon Institute (2023) [28-30]. Calculation of CAGR using the CAGR values in Table 5 and the standard growth-rate formula (Equation 1):

$$\left[\left(\frac{Final\ Value}{Initial\ Value}\right)^{\frac{1}{Number\ of\ Years}}\right] - 1 \quad (1)$$

The 28.3% growth in breaches underscores rapid threat escalation, especially relevant for policy planning. Regression outputs show significant negative coefficients for network security (-0.183, p=0.042) and infrastructure protection (-0.215, p=0.031), affirming their importance in breach mitigation. Application security lacks statistical significance, suggesting implementation lag or inefficiency. Ordinary Least Squares (OLS) regression analysis was conducted to assess the impact of cybersecurity spending on breach frequency, with results including coefficients and significance levels detailed in Table 6. OLS regression was used to test the hypothesis that higher security investment leads to fewer breaches. for network security (-0.183, p=0.042) and infrastructure protection (-0.215, p=0.031), affirming their importance in breach mitigation. Application security lacks statistical significance, suggesting implementation lag or inefficiency. Data breach numbers grew from 1001 in 2020 to 2116 in 2023. High standard deviation in malware and ransomware indicates their unpredictable nature, as shown in Table 7. The correlation matrix reveals phishing is most strongly associated with breaches (r=0.97). This substantiates the hypothesis that phishing is not just common but causally linked to serious breaches, justifying focused intervention (Table 8).

Figures 3 to 5 illustrate five key patterns:

1. Overall growth: The total volume of recorded cybersecurity events rose steadily from 5.6 billion incidents in 2020 to more than 7.1 billion in 2023, confirming an unabated upward trajectory.
2. Phishing and data breaches: Phishing incidents show a strong positive correlation with verified data breaches ($r = 0.97$, $p < 0.05$), underscoring the need for robust e-mail filtering and continuous user-awareness training.
3. Industry impact: Healthcare will have the highest average cost per cybersecurity incident at $10.93 million by 2023 (via Cybersecurity Ventures). This highlights the critical importance of defense-in-depth controls in highly regulated domains.
4. Ransomware: Ransomware volumes dipped slightly in 2022 but climbed again in 2023, suggesting attackers are recalibrating tactics rather than abandoning this lucrative vector.
5. DDoS resurgence: After a brief lull in 2021, DDoS attack frequency rebounded, pointing to adversaries' adoption of new amplification techniques and exploitation of fresh vulnerabilities.

These findings demonstrate that no industry is safe from cyberattacks, and ideally, there should be an overarching cybersecurity strategy across all organizations with added attention to critical sectors such as the healthcare and financial services industries [40-44].

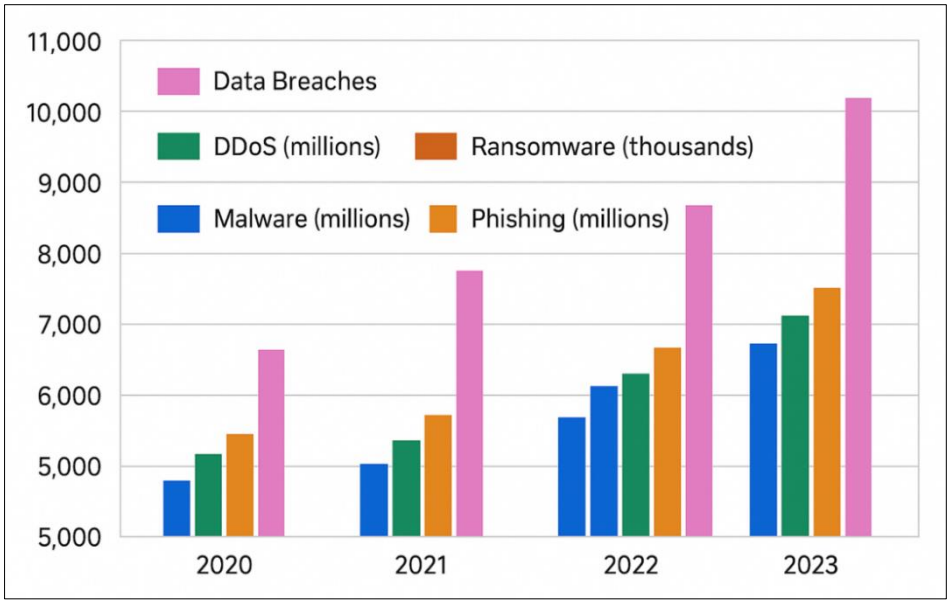

Figure 3. Cybersecurity Threat Landscape Evolution (2020-2023)

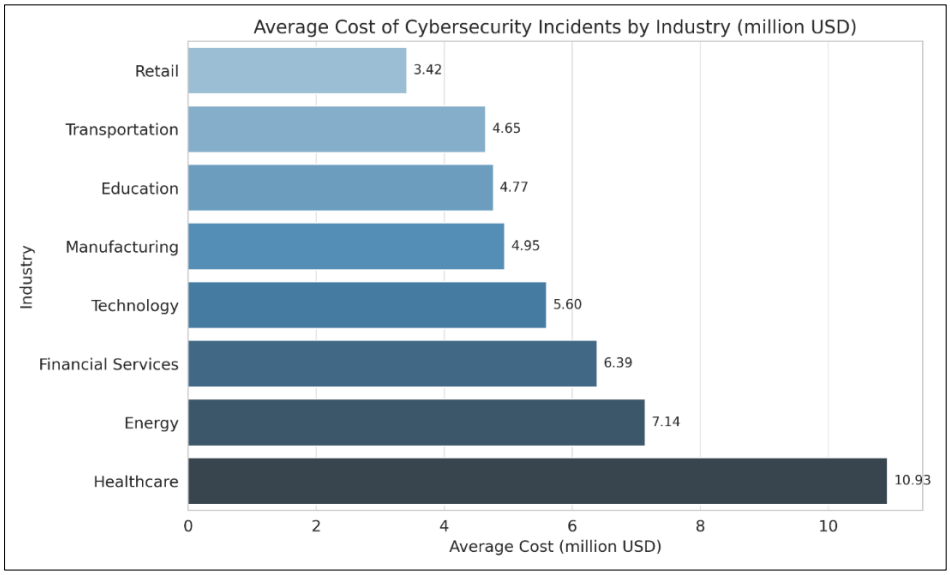

Figure 4. Average Cost of Data Breach by Industry (2023)

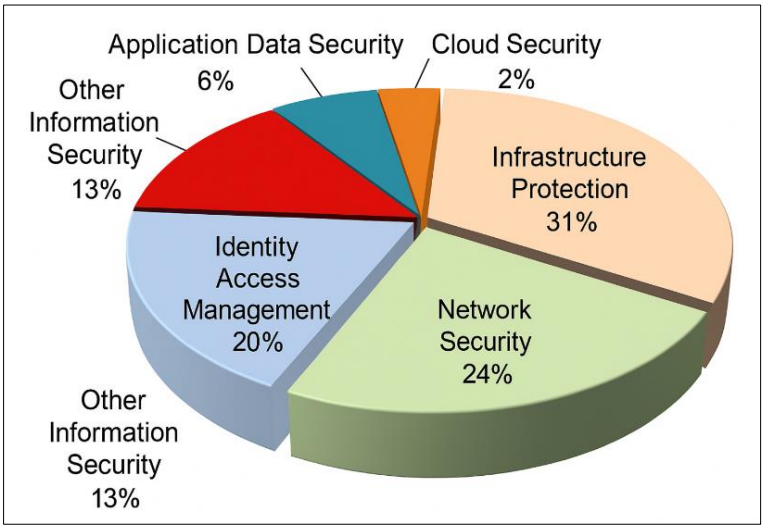

Figure 5. Cybersecurity Spending Distribution by Segment (2023)

4.1. Algorithm (Tkinter Python Code)

This algorithm builds a basic GUI for a cybersecurity risk assessment tool. It accepts user input for threat level, vulnerability level, and effect level, each on a scale of 1–10. It then produces a risk score and categorizes it into low, medium, or high risk. The program offers a basic framework for analyzing cybersecurity threats, which may be supplemented with more advanced algorithms and data inputs for a more thorough evaluation.

```
import tkinter as tk
from tkinter import messagebox
defcalculate_risk():
    try:
        threat = float(threat_entry.get())
        vulnerability = float(vulnerability_entry.get())
        impact = float(impact_entry.get())
        risk = (threat * vulnerability * impact) / 3
        if risk < 3:
risk_level = "Low"
elif 3 <= risk < 6:
risk_level = "Medium"
        else:
risk_level = "High"
result_label.config(text=f"Risk Score: {risk:.2f}\nRisk Level: {risk_level}")
    except ValueError:
messagebox.showerror("Error", "Please enter valid numeric values")
# Create main window
root = tk.Tk()
root.title("Cybersecurity Risk Assessment")
# Create and place widgets
tk.Label(root, text="Threat Level (1-10):").grid(row=0, column=0, padx=5, pady=5)
threat_entry = tk.Entry(root)
threat_entry.grid(row=0, column=1, padx=5, pady=5)
tk.Label(root, text="Vulnerability Level (1-10):").grid(row=1, column=0, padx=5, pady=5)
vulnerability_entry = tk.Entry(root)
vulnerability_entry.grid(row=1, column=1, padx=5, pady=5)
tk.Label(root, text="Impact Level (1-10):").grid(row=2, column=0, padx=5, pady=5)
impact_entry = tk.Entry(root)
impact_entry.grid(row=2, column=1, padx=5, pady=5)
calculate_button = tk.Button(root, text="Calculate Risk", command=calculate_risk)
calculate_button.grid(row=3, column=0, columnspan=2, pady=10)
result_label = tk.Label(root, text="")
result_label.grid(row=4, column=0, columnspan=2, pady=5)
root.mainloop()
```

4.2. Comparison with Studies

As summarized in Table 10, our study differs from prior work in timeframe, sectors covered, and statistical methods.

Table 10. Comparison of Current Study with Previous Research

Aspect	Current Study	Study A [37]	Study B [38]
Time Period	2020-2023	2018-2021	2019-2022
Geographic Focus	Global	North America	Europe
Industries Covered	8	5	6
Types of Attacks Analyzed	5	3	4
Statistical Methods	Correlation, Regression	Correlation	Time Series Analysis
Key Finding	Strong correlation between phishing and data breaches	Ransomware most costly	DDoS attacks on the rise

4.3. Research Gap

Although many studies have been carried out regarding trends in cybersecurity and their impact, a large research gap that remains unaddressed completely analyses the most recent data (2020–2023) from different angles, considering all areas of security. Prior research has focused on single types of cyber-attacks or specific sectors, which prevents a comprehensive view of the cybersecurity landscape. Moreover, there is no previous academic study that statistically investigates how various types of cyber risks are linked to their global economic implications for different sectors. Likewise, the return on security investment in addressing different types of assaults has received little attention, particularly with rapidly evolving threats and new tools to mitigate them. Furthermore, prior literature provides insufficient evidence to accurately depict how multiple weak signals interplay with one another to impact organizational postures regarding cyber security. This report attempts to address both of these deficits by providing an in-depth look at emerging cybersecurity themes, blending attack data (covering varied types), their financial implications, and the efficacy of security measures. It provides a much more complete picture of the current cybersecurity condition, which is necessary in order to be able to create successful strategies for dealing with increasing cyber threats.

5. Conclusion

Cyber threats are growing rapidly, with a CAGR of 28.3% for breaches alone between 2020 and 2023. Healthcare is the most financially affected industry, reinforcing the need for sector-specific resilience. A statistically significant link was found between phishing and breaches, highlighting the role of end-user behavior and email security. Regression results confirmed the effectiveness of targeted cybersecurity investments, particularly in infrastructure and network protection. Future work should examine emerging threats such as AI-enabled attacks and sectoral differences in regulatory compliance. Policymakers and business leaders must prioritize adaptive, data-informed strategies to mitigate cyber risks and ensure sustainable operational integrity.

5.1. Future Recommendation

The study's preliminary results point to eight clear avenues for advancing both academic research and frontline practice:

- Identify emerging threats. Track nascent vectors such as AI-generated attacks and quantum-enabled cryptographic breaks to ensure counter-measures keep pace.
- Measure AI / ML efficacy. Conduct head-to-head evaluations of machine-learning security platforms versus traditional defences to quantify detection□rate and false-positive trade-offs.
- Analyse human factors. Apply behavioral-economics lenses to security fatigue, risk compensation and training retention, then design evidence-based awareness programmes to close those gaps.
- Pursue sector-specific studies. Examine industry-unique vulnerabilities—particularly in healthcare, finance and critical infrastructure—to develop tailored mitigation frameworks.
- Assess regulatory impact. Empirically test how differing cybersecurity statutes, compliance regimes and enforcement levels affect organizational risk posture and breach incidence.
- Build predictive risk models. Leverage big-data analytics and threat-intelligence feeds to forecast attack likelihoods and prioritize controls dynamically.
- Quantify long-term economics. Undertake longitudinal studies on the macro-economic costs (and benefits) of cyber incidents to inform national-level policy and insurance pricing.
- Strengthen global collaboration. Explore mechanisms—such as shared threat-intelligence hubs and coordinated incident-response exercises—that enhance cross-border resilience.

These recommendations align directly with the patterns observed in our 2020-2023 dataset and address limitations noted in prior work, setting an agenda for a more resilient, data-driven cybersecurity ecosystem.

6. Declarations

6.1. Author Contributions

Conceptualization, S.A.H.H. and A.A.R.; methodology, S.A.H.H.; software, B.A.; validation, A.A.R. and Z.A.H.; formal analysis, S.A.H.H.; investigation, A.A.M.; resources, Z.A.H.; data curation, A.A.M.; writing—original draft preparation, S.A.H.H.; writing—review and editing, A.A.R. and B.A.; visualization, A.A.M.; supervision, B.A.; project administration, S.A.H.H.; funding acquisition, B.A. and S.A.H.H. All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available in the article.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Acknowledgments

We are grateful to the University of Misan for providing the necessary resources and support that enabled us to conduct this research.

6.5. Institutional Review Board Statement

Not applicable.

6.6. Informed Consent Statement

Not applicable.

6.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7. References

[1] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117. doi:10.3390/s23084117.

[2] Ketipov, R., Schnalle, R., Doukovska, L., & Dehez, D. (2024). Managing Cybersecurity: Digital Footprint Threats. Cybernetics and Information Technologies, 24(3), 151–162. doi:10.2478/cait-2024-0030.

[3] Dutta, V., & Zielińska, T. (2021). Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. Electronics (Switzerland), 10(22), 2850. doi:10.3390/electronics10222850.

[4] Jurišić, M., Tomičić, I., & Grd, P. (2023). User Behavior Analysis for Detecting Compromised User Accounts: A Review Paper. Cybernetics and Information Technologies, 23(3), 102–113. doi:10.2478/cait-2023-0027.

[5] Bogdanova, G., Todorov, T., & Georgieva-Tsaneva, G. (2018). Software approaches and methods to ensure the security of interactive systems. Cybernetics and Information Technologies, 18(5), 12–20. doi:10.2478/cait-2018-0017.

[6] Dasu, L. S., Dhamija, M., Dishitha, G., Vivekanandan, A., & Sarasvathi, V. (2023). Defending Against Identity Threats Using Risk-Based Authentication. Cybernetics and Information Technologies, 23(2), 105–123. doi:10.2478/cait-2023-0016.

[7] Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. Information and Computer Security, 29(5), 724–736. doi:10.1108/ICS-04-2020-0054.

[8] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. doi:10.1016/j.csa.2023.100031.

[9] Pemble, M. (2005). Evolutionary trends in bank customer-targeted malware. Network Security, 2005(10), 4–7. doi:10.1016/S1353-4858(05)70288-9.

[10] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176–8206. doi:10.1016/j.jksuci.2022.08.003.

[11] Pöyhönen, J., Simola, J., & Lehto, M. (2023). Basic Elements of Cyber Security for a Smart Terminal Process. International Conference on Cyber Warfare and Security, 18(1), 300–308. doi:10.34190/iccws.18.1.966.

[12] Pradeep Kumar, K., Prathap, B. R., Thiruthuvanathan, M. M., Murthy, H., & Jha Pillai, V. (2024). Secure approach to sharing digitized medical data in a cloud environment. Data Science and Management, 7(2), 108–118. doi:10.1016/j.dsm.2023.12.001.

[13] Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. Heliyon, 9(7), 17156. doi:10.1016/j.heliyon.2023.e17156.

[14] Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers and Security, 106, 102267. doi:10.1016/j.cose.2021.102267.

[15] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. doi:10.1016/j.jcss.2014.02.005.

[16] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability (Switzerland), 15(18), 13369. doi:10.3390/su151813369.

[17] Perwej, Y., Ahamad, F., Khan, M. Z., & Akhtar, N. (2021). An empirical study on the current state of internet of multimedia things (IoMT). International Journal of Engineering Research in Computer Science and Engineering, 8(3), 25-42.

[18] Cavelty, M. D. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Routledge, London, United Kingdom. doi:10.4324/9780203937419.

[19] GAO. (1996). Information Security: Computer Attacks at Department of Defense Pose Increasing Risks: Report to Congressional Requesters. General Accounting Office (GAO), AIMD-96-84. Available online: https://www.gao.gov/products/aimd-96-84 (accessed on May 2025).

[20] Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & security, 111, 102490.

[21] Lanza, C. (2022). Semantic control for the cybersecurity domain: investigation on the representativeness of a domain-specific terminology referring to lexical variation. CRC Press, New Jersey, United States.

[22] Easter, D. (2024). State Department cipher machines and communications security in the early Cold War, 1944–1965. Intelligence and National Security, 39(4), 620–635. doi:10.1080/02684527.2023.2269512.

[23] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186. doi:10.1016/j.egyr.2021.08.126.

[24] Oruj, Z. (2024). Cyber Security: contemporary cyber threats and National Strategies - Distance Education in Ukraine: Innovative, Normative-Legal. Pedagogical Aspects, 1(2), 100–116.

[25] Adigwe, C. S., Mayeke, N. R., Olabanji, S. O., Okunleye, O. J., Joeaneke, P. C., & Olaniyi, O. O. (2024). The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks. Asian Journal of Economics, Business and Accounting, 24(3), 289–306. doi:10.9734/ajeba/2024/v24i31287.

[26] CISA. (2023). Ransomware statistics. Cybersecurity& Infrastructure Security Agency, CISA. Available online: https://www.cisa.gov/stopransomware/fact-sheets-information (accessed on May 2025).

[27] Deloitte. (2023). Global healthcare cybersecurity report. Available online: https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html (accessed on May 2025).

[28] ENISA. (2023). Threat landscape report. European Union Agency for Cybersecurity, ENISA. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed on May 2025).

[29] IBM Security (2023). Cost of a data breach report 2023. Available online: https://www.ibm.com/reports/data-breach (accessed on May 2025).

[30] Ponemon Institute. (2023). The sixth annual global cyber risk report. Available online: https://www.ponemon.org/ (accessed on May 2025).

[31] Salman, I. R., Rasheed, A. A., Hassan, S. A. D. H., Hussein, R. A., & Al-Saady, M. (2025). Automated aquatic biodiversity monitoring using deep learning on the Tigris River: Species identification and ecosystem assessment. International Journal of Aquatic Biology, 13(1), 30–40. doi:10.22034/ijab.v13i1.2476.

[32] Rashid, M. K., Salman, I. R., Obaid, A. L., Hassan, S. A. D. H., Al-Musawi, M. R., & Al-Saady, M. (2024). Application of machine learning in predicting sources of water pollution in the Euphrates and Tigris rivers in Iraq. International Journal of Aquatic Biology, 12(6), 581–589. doi:10.22034/ijab.v12i6.2421.

[33] Hassan, S. A. D. H., Al-Furiji, H., Kareem Rashid, M., Abed Hussein, Z., & Ambudkar, B. (2024). Trending Algorithm on Twitter through 2023. Data and Metadata, 3, 384–384. doi:10.56294/dm2024384.

[34] Aboud, F. (2024). Flexural Behavior of Aligned Steel Reinforced Concrete Beams. Misan Journal of Engineering Sciences, 3(2), 197-213.

[35] Majeed, I. H. (2023). Experimental and Numerical Study of Torsional Solid and Hollow Section of Polyolefin Fiber-Reinforced Concrete Beams. Misan Journal of Engineering Sciences, 2(2), 71–84. doi:10.61263/mjes.v2i2.63.

[36] Khudhur, E., Aqeel H. Chkheiwer, & Adel A. Al Menhosh. (2023). Flexural Behavior of Normal and High Strength Self-Curing Self-Compacted Concrete Beams of Local Materials. Misan Journal of Engineering Sciences, 2(1), 98-124. doi:10.61263/mjes.v2i1.47.

[37] Smith, A. (2022). The cybersecurity threat landscape in 2022: A focus on critical infrastructure. Security Journal, 11(3), 245–262.

[38] Jones, T. (2023). The financial impact of cybercrime on the healthcare industry - Journal of Medical Economics, 26(7), 891-898.

[39] Mousa, A. A., Hassan, S. A. D. H., Rashid, M. K., & Al-Saady, M. (2025). Safeguarding Patient Data: Machine Learning for Phishing URL Detection in Healthcare Systems. Journal of Advanced Research Design, 131(1), 47–60. doi:10.37934/ard.131.1.4760.

[40] Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. Future Generation Computer Systems, 98, 660-671. doi:10.1016/j.future.2019.03.042.

[41] Shackell, M., & Leader, F. S. (2005). Global Economic Crime Survey. PwC, London, United Kingdom

[42] Alanazi, A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. Cureus, 15(10), 47026. doi:10.7759/cureus.47026.

[43] Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. International Journal of Information Management, 74, 102719. doi:10.1016/j.ijinfomgt.2023.102719.

[44] Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering, 345–404. doi:10.1007/978-3-319-95669-5_10.