© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

Cybersecurity of Critical Infrastructures: Challenges, Empirical Threat Analytics and Future Resilience Perspectives

KEN MUDZINGWA[1], STEWART MUNYARADZI NYAMUTSWA[2], ADMORE TAFADZWA MUGWADZI[3], PANASHE YOLANDA DHEGWA[4], MUNASHE NAPHTALI MUPA[5]

[1]*Yeshiva University, ORCiD: 0009-0005-1090-6492*

[2]*Yeshiva University, ORCiD: 0009-0009-2710-2617*

[3]*St Thomas University, ORCiD: 0009-0000-1501-0840*

[4]*University of Nevada Las Vegas, ORCiD: 0009-0002-3681-2804*

[5]*Hult International Business School, ORCiD: 0000-0003-3509-861X*

Abstract- ***Critical infrastructure now depends on cloud platforms, 5G-enabled connectivity, operational technology, Internet of Things devices and data-intensive service delivery. This convergence has widened the attack surface for essential sectors such as energy, water, telecommunications, healthcare, banking, government and transportation. Building on critical-infrastructure cybersecurity scholarship and using a structured public incident dataset of 3,000 records covering 2015-2024, this paper develops an empirical picture of cyber risk across attack types, industries, countries, vulnerability classes and defensive mechanisms. The analysis shows that the sample records an aggregate estimated financial exposure of USD 151.48 billion, an average incident loss of USD 50.49 million, approximately 1.51 billion affected-user records and a mean resolution time of 36.48 hours. DDoS and phishing appear as the most frequent attack categories, while the IT, banking and healthcare sectors carry the largest incident counts. Heat-map analysis identifies Government-DDoS, Telecommunications-Man-in-the-Middle and IT-Man-in-the-Middle combinations as notable high-risk cells under a composite impact measure combining financial loss, affected users and incident resolution time. Statistical tests show weak direct association between categorical attack labels and loss severity, implying that omitted variables such as asset criticality, control maturity, identity exposure, network segmentation, patch latency, vendor concentration and incident-response capability may be more decisive than sector labels alone. The paper therefore proposes a risk-based Critical Infrastructure Cyber Resilience Framework built around governance, asset visibility, zero-trust identity, vulnerability prioritisation, AI-assisted detection, supply-chain assurance, incident reporting and recovery engineering. The contribution is both empirical and practical: it provides an applied analytics model for prioritising critical-infrastructure cyber risk and a governance architecture aligned with NIST CSF 2.0 and contemporary critical-infrastructure protection requirements.***

Keywords: ***critical infrastructure; cybersecurity; 5G security; cloud security; cyber resilience; ransomware; DDoS; vulnerability management; NIST CSF; cyber risk analytics.***

I. INTRODUCTION

Critical infrastructure is no longer a collection of isolated physical assets. It is a connected socio-technical system made up of networks, cloud services, operational technology, sensors, identity services, data platforms, vendors and human operators. This architecture creates new forms of efficiency, but it also changes the logic of cyber risk. A compromise in one layer can cascade into service interruption, public-safety harm, privacy loss, regulatory exposure and economic damage. The national importance of cybersecurity therefore lies not only in protecting data but also in sustaining the continuity of essential services.

The policy context has shifted in the same direction. The United States Government Accountability Office has described the protection of critical infrastructure such as water and electricity from cyberattacks as a national priority and noted that the nation's 16 critical infrastructure sectors rely on electronic systems to provide essential services including

electricity, communications and financial services (GAO, 2023). NIST Cybersecurity Framework 2.0 similarly expands cybersecurity risk management from a purely technical control activity into a governance, communication and enterprise-risk discipline designed for organisations of all sizes and sectors (NIST, 2024).

The technical context is equally important. 5G, cloud computing, edge computing and IoT are rapidly being integrated into industrial and public-service environments. While these technologies enable automation, real-time analytics and remote service delivery, they also introduce network slicing risks, API exposure, identity sprawl, cloud misconfiguration, supply-chain dependency, and complex interactions between information technology (IT) and operational technology (OT). In such environments, the defender must protect not merely endpoints but also trust relationships across distributed systems.

This article responds to that problem by combining literature-based cybersecurity analysis with a structured empirical examination of cyber incidents. It is grounded in the article by Maglaras, Janicke and Ferrag (2022), which frames cybersecurity of critical infrastructures as a systems challenge requiring resilient technical and organisational responses. It also extends recent work on adaptive cybersecurity, graph-based security modelling and AI-enabled risk management by focusing on measurable incident patterns and practical prioritisation logic (Moyo, Zhuwankinyu and Mupa, 2024; Zhuwankinyu, Mupa and Tafirenyika, 2025; Aror and Mupa, 2025).

II. PROBLEM STATEMENT AND RESEARCH QUESTIONS

Critical-infrastructure cybersecurity decisions are often made under pressure, with incomplete information and competing priorities. Boards, technology leaders and security teams need a way to translate heterogeneous cyber incidents into actionable risk priorities. Yet many organisations still rely on broad threat labels such as ransomware, DDoS or phishing without linking them to sector exposure, financial impact, affected users, vulnerability conditions, defence mechanisms and incident-resolution speed. This creates a governance gap: leaders may invest heavily in visible threats while underinvesting in the systemic conditions that make incidents costly and difficult to contain.

The central research question is: how can structured cyber-incident analytics improve the prioritisation of critical-infrastructure cybersecurity controls in cloud-connected and 5G-enabled environments? The supporting questions are:

- Which sectors, attack types, countries and vulnerability classes show the highest incident volume and estimated financial exposure in the analytical sample?
- Which sector-attack combinations produce the highest composite risk when financial loss, affected users and resolution time are considered together?
- Do categorical attack labels statistically explain financial-loss severity, or do the results suggest that omitted control and asset-criticality variables are decisive?
- What governance and control framework should critical-infrastructure operators adopt to convert threat intelligence into measurable resilience?

III. LITERATURE REVIEW

3.1 Critical infrastructure as a cyber-physical risk system

Critical infrastructure differs from ordinary enterprise IT because its failure can affect public safety, economic stability, health services, national security and social trust. Cyber-physical systems literature emphasises that these environments combine computation, communication and physical processes, making confidentiality, integrity, availability and safety interdependent (Humayed et al., 2017). Industrial control systems add further constraints: long asset lifecycles, availability requirements, legacy protocols, vendor-specific devices and operational safety considerations make simple patch-and-replace models impractical (Nankya et al., 2023). Maglaras, Janicke and Ferrag (2022) argue that critical-infrastructure cybersecurity requires solutions

across technology, policy, governance and resilience. Their work is important because it moves beyond a narrow perimeter-security model and recognises that critical infrastructure depends on dynamic cyber-physical environments. In this paper, that logic is translated into a data-driven prioritisation model: the objective is not simply to list threats, but to identify which threat-sector combinations are most likely to create material operational and financial consequences.

3.2 Cloud, 5G, edge and IoT convergence

Cloud and 5G architectures are central to modern critical-infrastructure operations. 5G network slicing enables differentiated service quality and resource isolation but creates new attack surfaces in orchestration, virtualisation, slice isolation and lifecycle management (Ordonez-Lucena et al., 2017; Barakabitze et al., 2020; De Alwis et al., 2024). Cloud platforms introduce scale and resilience, but they also depend heavily on identity, configuration management, API control, logging, encryption and third-party service assurance.

This convergence changes cybersecurity from a perimeter issue into a shared-responsibility and trust-management problem. A compromised cloud identity can become an entry point into data lakes, customer records, operational dashboards or vendor-integrated systems. A vulnerable IoT device can become a pivot point into industrial networks. A 5G slice that is poorly isolated can expose traffic or management planes. For critical infrastructure, these risks are systemic because service continuity depends on the integrity of many interconnected layers.

3.3 Ransomware, DDoS, vulnerability exploitation and incident economics

Current threat-landscape reporting consistently identifies ransomware, DDoS, vulnerability exploitation, credential misuse and social engineering as persistent threats. ENISA (2024) highlights ransomware and threats against availability, including DDoS, as top threat types. Verizon (2024) reports a major rise in vulnerability exploitation as a critical path into breaches, particularly in the context of ransomware and extortion. IBM (2025) estimates the global average cost of a data breach at USD 4.4 million and highlights the growing importance of AI governance, identity security, data security, security automation and resilience.

Financial loss in cyber incidents is rarely determined by attack type alone. It is mediated by the value of affected data, dependency of operations on the compromised system, regulatory requirements, insurance coverage, public communication, recovery time, maturity of incident response, cloud architecture, supply-chain concentration and the quality of backups. This is why descriptive analytics must be combined with governance interpretation. An attack type that appears average in raw frequency may still be strategically critical if it targets high-dependency operational assets.

3.4 Adaptive cybersecurity, AI and graph-based risk management

Recent scholarship increasingly focuses on adaptive cybersecurity and AI-assisted defence. Moyo, Zhuwankinyu and Mupa (2024) argue that generative AI can support adaptive enterprise cybersecurity policies, real-time threat detection and automated response-pattern development. Zhuwankinyu, Mupa and Tafirenyika (2025) extend the discussion through graph-based security models for AI-driven data storage, emphasising anomaly detection, relationship mapping, cryptographic integrity and future security frameworks enriched by AI and quantum-safe methods. Aror and Mupa (2025) further link AI to corporate risk management and compliance, noting the value of predictive analytics, real-time monitoring and governance transparency.

These contributions are directly relevant to critical-infrastructure protection because traditional control checklists do not scale well in environments with thousands of assets, multiple vendors, distributed identities and constantly changing vulnerabilities. Graph models can represent relationships among users, devices, applications, data stores and network segments. AI-assisted detection can identify anomalous behaviours that static signatures miss. However, AI must be governed. Without explainability, data quality, access controls and accountability, AI can create new risks rather than reduce existing ones.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

IV. DATA AND METHODOLOGY

4.1 Data source

The empirical component uses the public Global Cybersecurity Threats (2015-2024) dataset originally listed on Kaggle and accessed through a public GitHub mirror of the Kaggle dataset. The file contains 3,000 incident observations and ten primary fields: country, year, attack type, target industry, financial loss in million U.S. dollars, number of affected users, attack source, security vulnerability type, defence mechanism used and incident-resolution time in hours. The dataset is suitable for exploratory threat-intelligence analytics, comparative sector analysis and demonstration of risk-prioritisation workflows. Because public incident datasets are not equivalent to regulated breach-reporting records, findings are interpreted as structured analytical indicators rather than definitive national breach statistics.

Table 1. Dataset schema and operational interpretation

Variable	Operational meaning	Type
Country	Country where the attack occurred	Categorical
Year	Year of incident, 2015-2024	Integer
Attack Type	DDoS, phishing, ransomware, malware, SQL injection or man-in-the-middle	Categorical
Target Industry	Sector affected by the incident	Categorical
Financial Loss (in Million $)	Estimated financial loss in USD million	Numeric
Number of Affected Users	Number of users or records affected	Numeric
Attack Source	Insider, nation-state, hacker group or unknown	Categorical
Security Vulnerability Type	Zero-day, weak passwords, unpatched software or social engineering	Categorical
Defense Mechanism Used	Antivirus, firewall, VPN, encryption or AI-based detection	Categorical
Incident Resolution Time (in Hours)	Containment/resolution time in hours	Numeric

4.2 Analytical design

The analysis proceeded in five stages. First, data quality checks confirmed the number of observations, variable types and missing values. Second, descriptive statistics were calculated for incident frequency, financial loss, affected users and incident-resolution time. Third, pivot-table heat maps were generated to visualise average financial loss, composite risk and incident counts across sector, attack type, country, vulnerability type and defence mechanism. Fourth, non-parametric statistical tests were applied because the outcome variables were not assumed to be normally distributed: chi-square testing examined the association between attack type and target industry; Kruskal-Wallis tests compared financial-loss distributions across major categorical variables; and Spearman rank correlations examined relationships between financial loss, affected users, resolution time and year. Fifth, a random-forest classifier was trained to predict whether an incident fell in the top quartile of a composite risk score. A separate random-forest regression tested whether observable labels could predict financial loss directly. The composite risk score was defined as follows:

$$\text{Composite Risk} = 0.45(z\ \text{Financial Loss}) + 0.35(z\ \text{Affected Users}) + 0.20(z\ \text{Resolution Time})$$

The weights reflect the analytical priority of direct financial severity, scale of human or customer exposure, and duration of operational disruption. The score is not presented as a universal formula; it is a transparent decision-support measure that can be recalibrated for sectors where safety, service continuity or regulatory reporting are more important than financial loss alone.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

V. RESULTS

5.1 Dataset completeness and descriptive profile

The analytical file contains 3,000 records and no missing values across the ten primary variables. The sample covers ten countries, six attack types, seven target industries, four vulnerability classes and five defence mechanisms. Estimated financial loss ranges from USD 0.50 million to USD 99.99 million. The mean estimated loss is USD 50.49 million, while the median is USD 50.80 million. The total financial exposure in the sample is USD 151.48 billion, and the aggregate affected-user count is 1,514,052,409.

Table 2. Overall impact statistics for the analytical sample

Metric	n	Mean	Median	Std. dev.	Minimum	Maximum	Total
Financial Loss (in Million $)	3,000.00	50.49	50.80	28.79	0.50	99.99	151,478.91
Number of Affected Users	3,000.00	504,684.14	504,513.00	289,944.08	424.00	999,635.00	1,514,052,409.00
Incident Resolution Time (in Hours)	3,000.00	36.48	37.00	20.57	1.00	72.00	109,428.00

5.2 Annual incident and loss pattern

Incident counts fluctuate across the decade rather than following a monotonic trend. The highest annual incident count in the dataset occurs in 2017, followed closely by 2022, 2020 and 2023. Estimated annual financial loss peaks in 2017, 2023, 2021 and 2022. These patterns should not be interpreted as confirmed global incidence rates; rather, they show that the sample has sufficient temporal coverage to support trend analysis and risk-dashboard design.

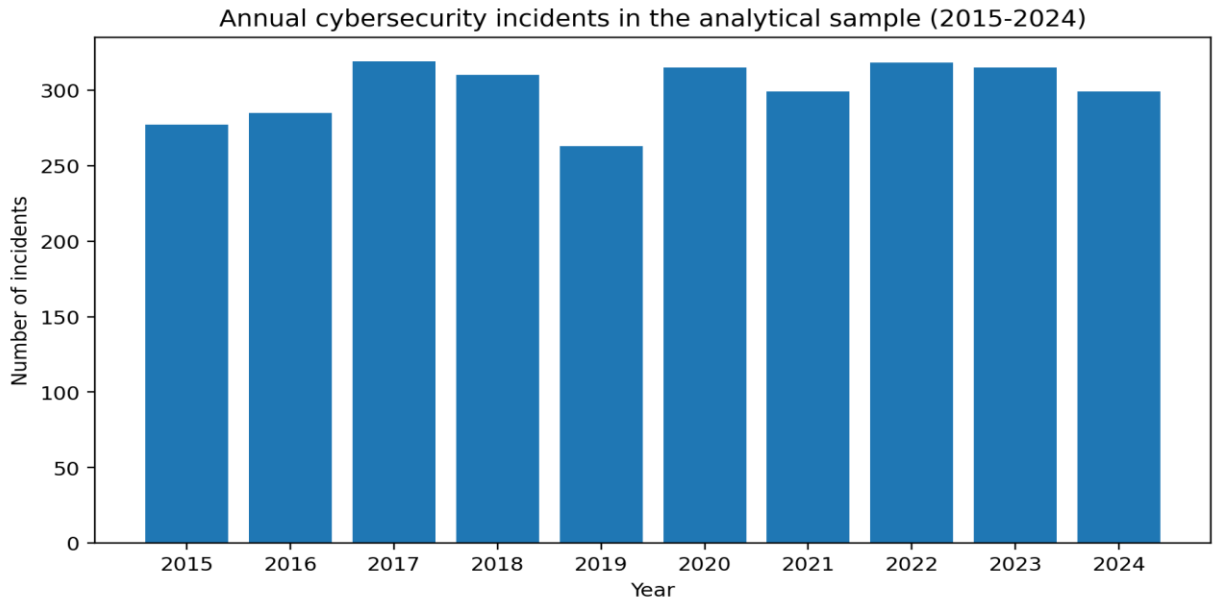

Figure 1. Annual cybersecurity incident count in the analytical sample.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

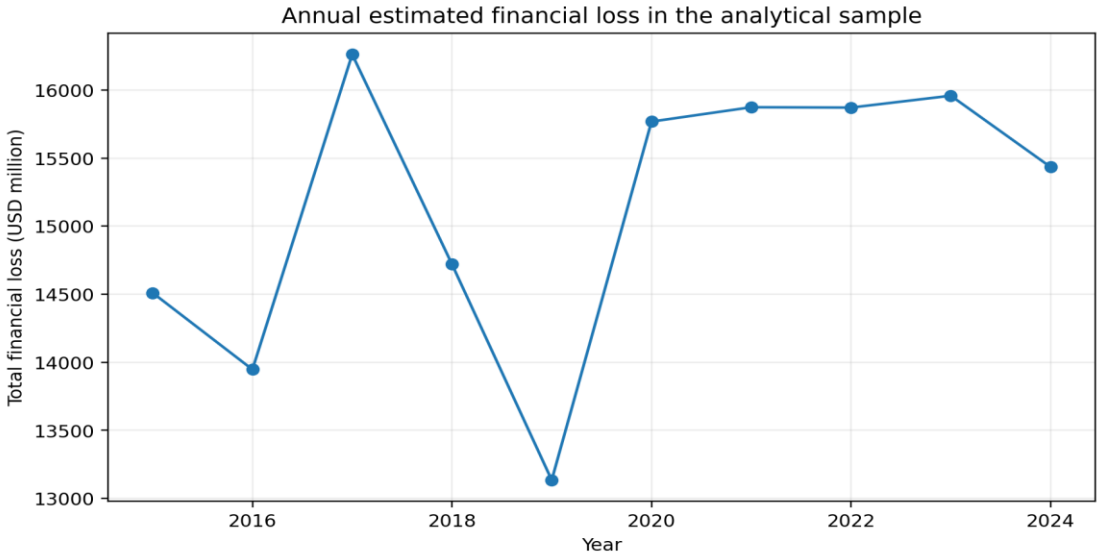

Figure 2. Annual estimated financial loss in USD million.

5.3 Sector and attack-type exposure

The IT sector records the highest incident count and highest total estimated loss, followed by banking. Government has a lower incident count than IT and banking but a higher mean loss per incident than several other sectors. This is consistent with the critical-infrastructure argument that risk is not only a volume problem: the strategic importance of the affected assets determines the seriousness of an incident.

Table 3. Sector-level incident exposure, financial loss and operational impact

Target Industry	Incidents	Total loss USD m	Mean loss USD m	Mean affected users	Mean resolution hours	Mean risk score
IT	478	24,809.83	51.90	523,210.94	36.17	0.04
Banking	445	22,772.39	51.17	505,839.11	35.74	0.00
Government	403	21,205.33	52.62	499,352.43	37.59	0.04
Retail	423	21,119.55	49.93	488,833.06	37.22	-0.02
Healthcare	429	21,041.29	49.05	504,130.34	35.81	-0.03
Telecommunications	403	20,459.09	50.77	495,203.75	37.06	-0.00
Education	419	20,071.43	47.90	513,137.79	35.91	-0.04

DDoS and phishing are the two most frequent attack types in the dataset. DDoS also has the highest total estimated financial loss, while man-in-the-middle attacks have the highest average affected-user count. These results support the need to protect both availability and confidentiality. Availability threats affect continuity of operations, while interception and credential-centred attacks can compromise trust relationships and sensitive data across interconnected infrastructure layers.

Table 4. Attack-type exposure and impact metrics

Attack Type	Incidents	Total loss USD m	Mean loss USD m	Mean affected users	Mean resolution hours	Mean risk score
DDoS	531	27,630.92	52.04	499,437.41	35.69	0.01

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

Phishing	529	26,693.29	50.46	487,179.54	35.91	-0.03
SQL Injection	503	25,156.56	50.01	512,469.83	36.91	0.01
Ransomware	493	24,479.32	49.65	502,825.37	36.53	-0.01
Malware	485	23,967.95	49.42	508,780.23	37.07	-0.01
Man-in-the-Middle	459	23,550.87	51.31	520,064.32	36.87	0.04

5.4 Heat-map analysis

The average-loss heat map reveals concentration patterns that would be less visible in a flat table. Government-DDoS incidents show the highest average financial loss among major sector-attack combinations. Banking-DDoS and IT-ransomware also show elevated mean losses. The interpretation is practical: critical-infrastructure leaders should not build programmes around generic controls only; they should map attack types to business services and operational dependencies.

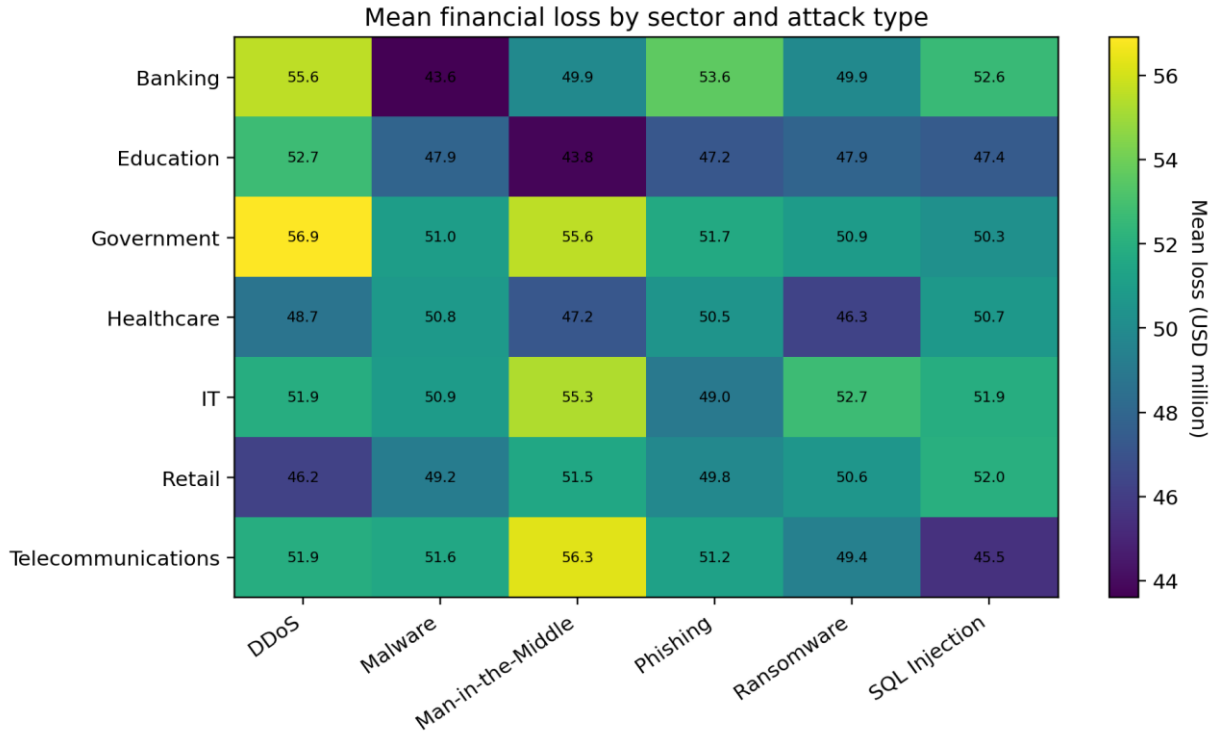

Figure 3. Heat map of mean financial loss by target industry and attack type.

The composite-risk heat map incorporates not only financial loss but also affected users and resolution time. Under this measure, the top high-risk cells are Government-DDoS, Telecommunications-Man-in-the-Middle, IT-Man-in-the-Middle, IT-DDoS and Government-Man-in-the-Middle. This result is significant for 5G and cloud-connected infrastructure because telecommunications and IT act as enabling layers for other critical sectors. A compromise in these sectors can transmit risk into healthcare, banking, government services and emergency communications.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

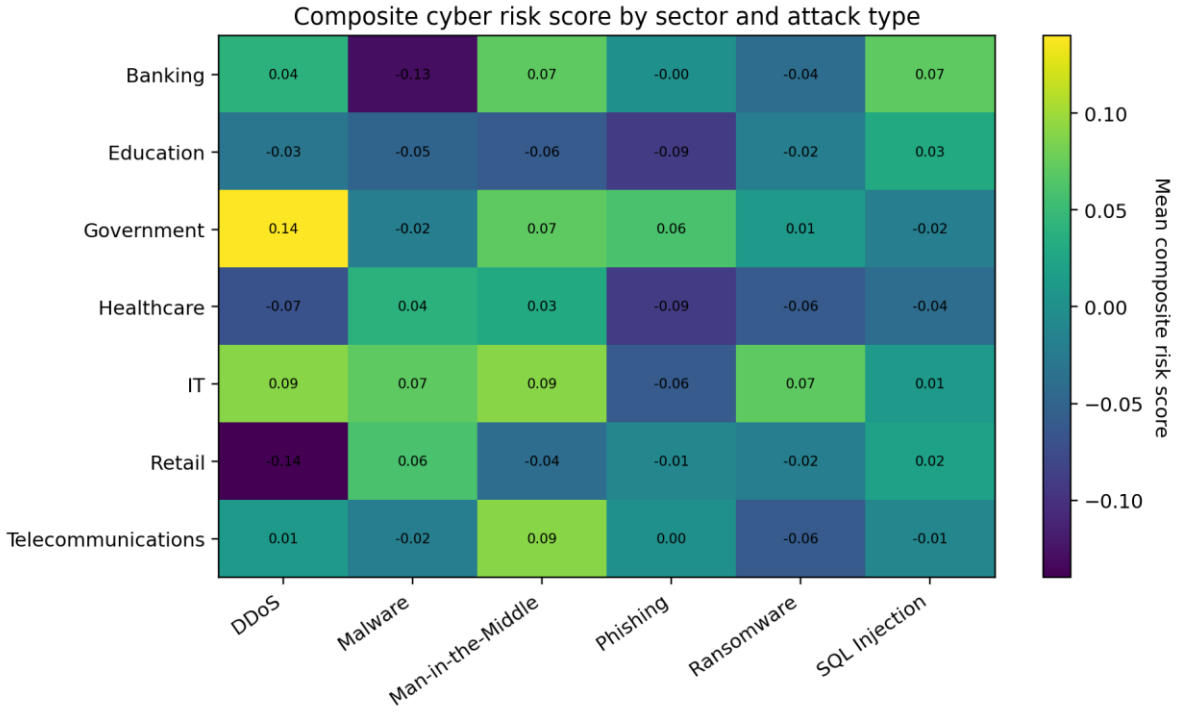

Figure 4. Heat map of composite cyber risk score by target industry and attack type.

Table 5. Top 10 sector-attack combinations by composite risk score

Target Industry	Attack Type	Incidents	Total loss USD m	Mean loss USD m	Mean affected users	Mean resolution hours	Mean risk score
Government	DDoS	71	4,041.50	56.92	511,390.24	39.37	0.14
Telecommunications	Man-in-the-Middle	56	3,150.10	56.25	517,250.43	34.59	0.09
IT	Man-in-the-Middle	80	4,421.12	55.26	529,193.75	34.67	0.09
IT	DDoS	91	4,718.88	51.86	560,951.19	36.12	0.09
Government	Man-in-the-Middle	53	2,947.30	55.61	492,063.55	37.42	0.07
IT	Ransomware	74	3,902.29	52.73	537,515.51	36.26	0.07
IT	Malware	67	3,411.47	50.92	540,373.01	38.34	0.07
Banking	Man-in-the-Middle	77	3,839.39	49.86	535,860.74	40.57	0.07
Banking	SQL Injection	71	3,737.49	52.64	529,349.17	36.68	0.07
Government	Phishing	68	3,516.48	51.71	514,186.68	39.34	0.06

Country-attack mapping provides a second layer of situational awareness. The heat map does not imply country-level culpability or national risk ranking; rather, it shows how a threat-intelligence dashboard can compare geographical exposure in a multi-country dataset. In operational use, such a dashboard would be enriched with reporting quality, sector mix, threat actor activity, geopolitical context and supply-chain dependence.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

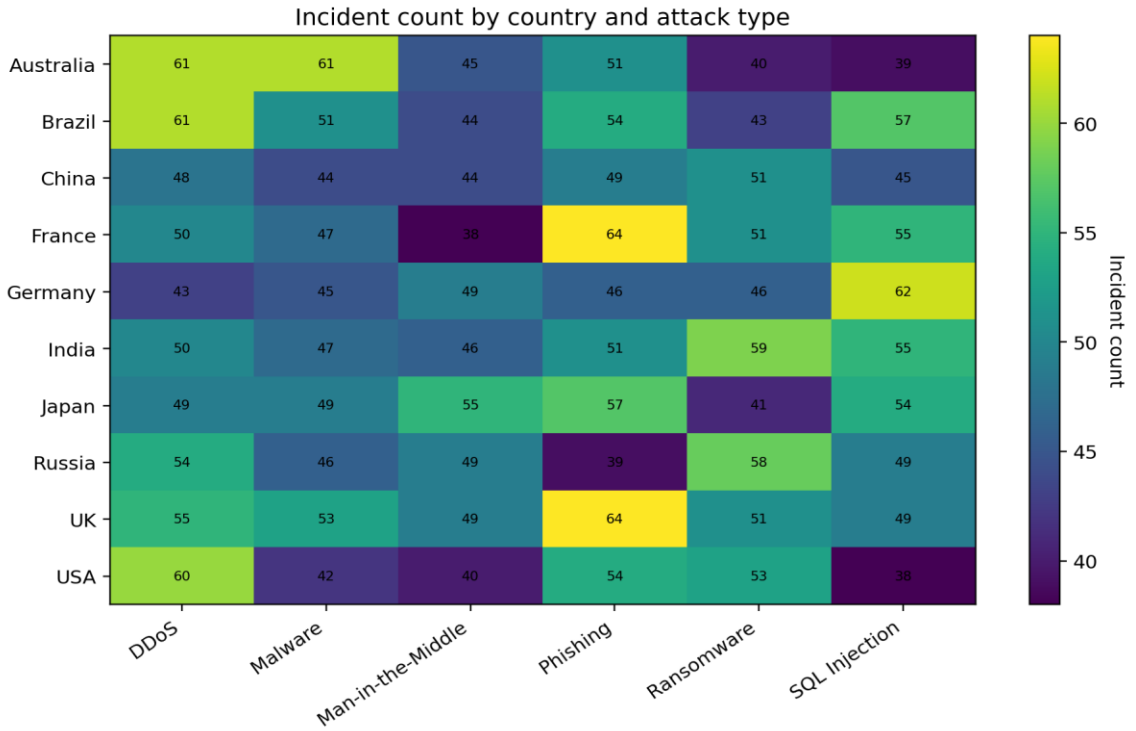

Figure 5. Heat map of incident count by country and attack type.

The vulnerability-defence heat map shows mean resolution time by vulnerability class and defence mechanism. Unpatched-software incidents show the highest average resolution time overall, which is consistent with the practical difficulty of remediating technical debt in production environments. The result also explains why vulnerability prioritisation should not be based on CVSS severity alone; exploited status, asset criticality, compensating controls, network exposure and operational constraints should also be considered.

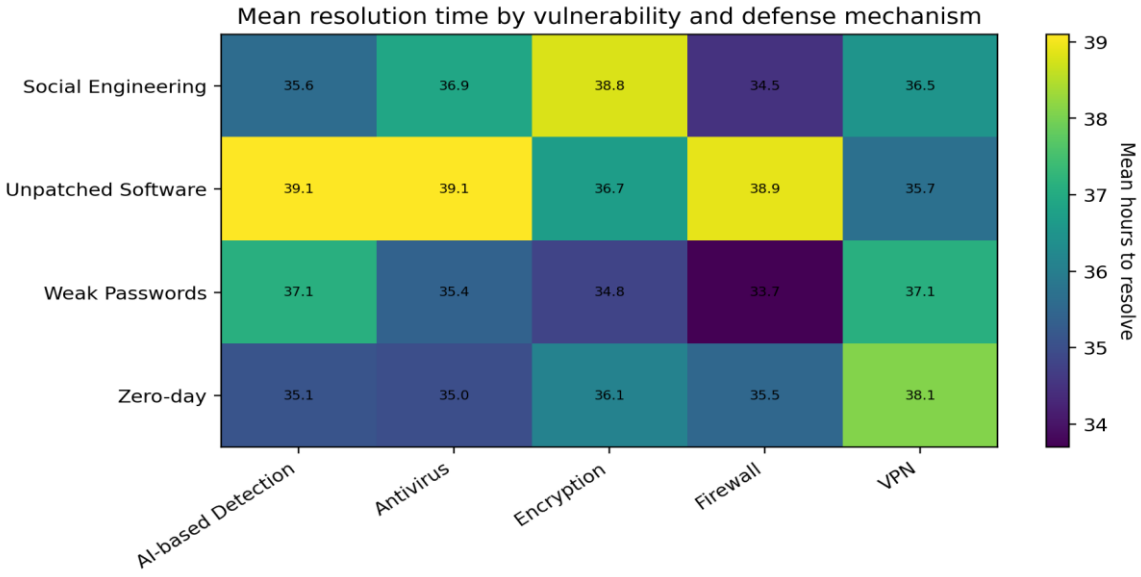

Figure 6. Heat map of mean resolution time by vulnerability type and defence mechanism.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

5.5 Statistical tests and model results

The chi-square test for association between attack type and target industry produced $X^2=38.46$, df=30 and p=0.138. This indicates no statistically significant association at the 5% level in this analytical sample. Kruskal-Wallis tests also did not find statistically significant differences in financial-loss distributions by target industry (H=8.17, p=0.226), attack type (H=3.19, p=0.671), defence mechanism (H=1.62, p=0.805) or vulnerability type (H=0.28, p=0.965). Spearman correlations between financial loss and affected users (rho=0.002, p=0.924), resolution time (rho=-0.013, p=0.485) and year (rho=0.011, p=0.563) are also weak.

The modelling results reinforce the same point. A random-forest regression attempting to predict financial loss from the available incident labels produced a mean absolute error of USD 25.15 million and an R^2 of -0.028, indicating weak explanatory power. By contrast, the high-risk quartile classifier achieved AUC=0.827, accuracy=0.775 and F1=0.561 because the composite label incorporates affected users and resolution time. Feature importance places affected users, incident resolution time and year above most categorical labels. The result is not a claim that financial loss is unpredictable in general; rather, it shows that richer asset-level variables are needed to model incident severity properly.

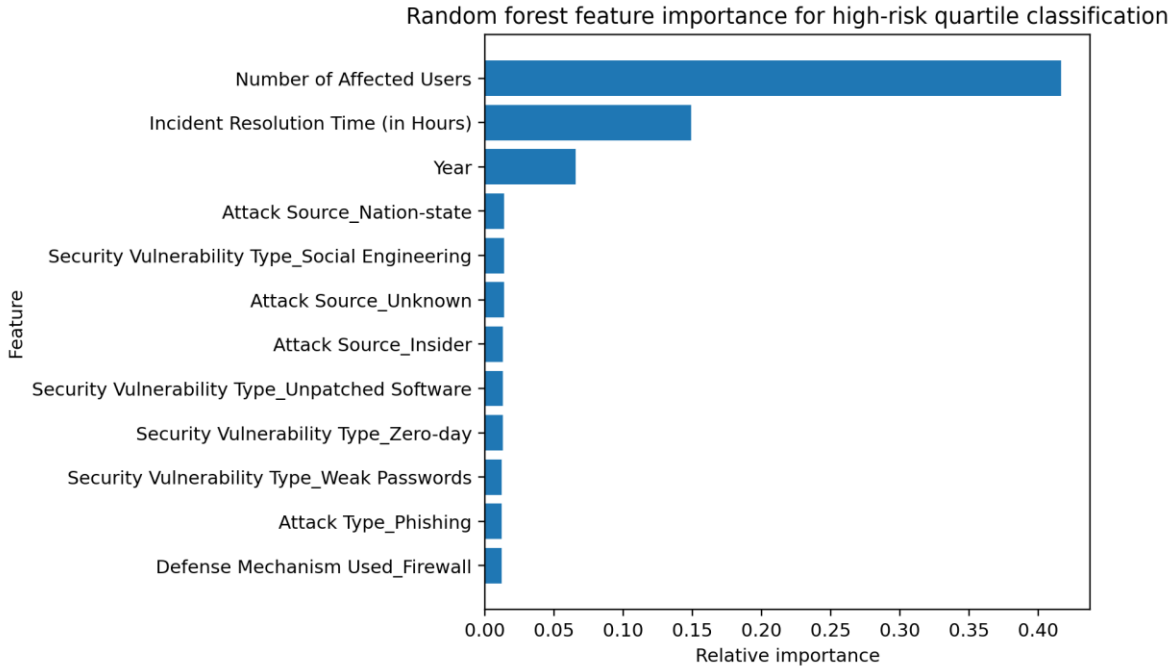

Figure 7. Random-forest feature importance for high-risk quartile classification.

Table 6. Top feature importances for high-risk quartile classification

Feature	Importance
Number of Affected Users	0.4167
Incident Resolution Time (in Hours)	0.1492
Year	0.0655
Attack Source_Nation-state	0.0141
Security Vulnerability Type_Social Engineering	0.0140
Attack Source_Unknown	0.0139
Attack Source_Insider	0.0133
Security Vulnerability Type_Unpatched Software	0.0130
Security Vulnerability Type_Zero-day	0.0130

Security Vulnerability Type_Weak Passwords	0.0123
Attack Type_Phishing	0.0123
Defense Mechanism Used_Firewall	0.0122

VI. DISCUSSION

6.1 What the empirical results mean for critical infrastructure

The empirical results support three important conclusions. First, attack labels are useful for situational awareness but insufficient for investment prioritisation. DDoS, phishing, ransomware and man-in-the-middle attacks matter, but the real question is which business services, data stores, identities, vendors and operational dependencies they affect. Second, financial-loss severity cannot be adequately explained by broad sector and attack categories alone. This strengthens the case for asset-centric cyber risk analytics that include asset criticality, exposure, control maturity, identity privileges, vendor dependency, exploitable vulnerabilities and incident-response readiness. Third, composite metrics provide more actionable insight than single-variable dashboards because they integrate financial, human and operational dimensions of impact.

For critical infrastructure, the highest-risk combinations are not always the most frequent incidents. Government-DDoS and telecommunications interception-type attacks are strategically important because they affect public trust, continuity of essential services and the integrity of communications. IT-sector incidents are also systemic because IT is not only a sector; it is a dependency layer for other sectors. This supports a resilience perspective in which cybersecurity is treated as a continuity, governance and public-value function rather than merely an IT function.

6.2 Implications for 5G, cloud and edge security

The integration of 5G, cloud and edge systems intensifies the need for identity-centred and data-centred controls. In 5G-enabled infrastructure, software-defined networking, network slicing, virtual network functions, edge workloads and API-based orchestration reduce the usefulness of static perimeter models. Security teams must therefore monitor control-plane activity, enforce slice isolation, validate workload identity, encrypt sensitive traffic, control privileged access and continuously assess cloud configuration drift.

Cloud security must also be reframed as resilience engineering. The objective is not only to prevent compromise but also to maintain service continuity under degraded conditions. This requires immutable backups, tested recovery plans, incident runbooks, multi-region failover, security logging, detection engineering and business-impact analysis tied directly to critical services. Where cloud services support OT or public-service operations, organisations should define recovery time objectives and recovery point objectives at the service level rather than at the generic server level.

6.3 The role and limits of AI-assisted defence

AI-assisted detection and automated response are valuable because critical-infrastructure environments generate too much telemetry for purely manual analysis. Behavioural analytics, graph-based anomaly detection, natural-language policy mapping and automated enrichment of threat intelligence can shorten detection and triage cycles. This aligns with recent work arguing that generative AI and graph-based security models can strengthen adaptive security policies and real-time anomaly detection (Moyo, Zhuwankinyu and Mupa, 2024; Zhuwankinyu, Mupa and Tafirenyika, 2025).

However, AI cannot substitute for governance. AI models require access controls, quality data, explainability, human oversight and audit trails. IBM (2025) highlights that organisations without AI governance and proper AI access controls face increased exposure. For critical infrastructure, the standard must be higher: AI-driven security recommendations should be explainable to analysts, auditable by governance teams and aligned with legally defensible incident-response procedures.

© AUG 2026 | IRE Journals | Volume 10 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I2-1722430

VII. PROPOSED CRITICAL INFRASTRUCTURE CYBER RESILIENCE FRAMEWORK

Based on the literature and empirical analysis, this paper proposes a Critical Infrastructure Cyber Resilience Framework (CICRF) with eight mutually reinforcing pillars. The framework is designed to be implemented as an enterprise programme rather than as a narrow technical control list.

Table 7. Critical Infrastructure Cyber Resilience Framework (CICRF)

Pillar	Core controls	Primary risk addressed
1. Governance and accountability	Board-level cyber-risk ownership; defined risk appetite; cybersecurity integrated into enterprise risk management; reporting aligned with NIST CSF 2.0 Govern function.	Governance gap; weak ownership; fragmented decision-making
2. Asset and dependency visibility	Inventory of IT, OT, cloud, IoT, identities, vendors, APIs and critical business services; dependency maps for crown-jewel services.	Unknown exposure; unmonitored assets; hidden dependencies
3. Zero-trust identity and access	Least privilege, phishing-resistant MFA, privileged-access management, workload identity, continuous authentication and segmentation.	Credential theft; lateral movement; overprivileged accounts
4. Vulnerability and exposure prioritisation	Use CVSS, EPSS, CISA KEV, exploit activity, asset criticality, internet exposure and compensating controls to prioritise remediation.	Patch backlogs; unpatched software; zero-day exposure
5. Detection engineering and AI-assisted analytics	Telemetry pipelines, SIEM/SOAR use cases, behavioural analytics, graph-based anomaly detection and explainable alert triage.	Delayed detection; alert fatigue; stealthy adversary movement
6. Cloud, 5G and edge hardening	Secure configuration baselines, API security, slice isolation, encryption, logging, cloud posture management and edge workload control.	Cloud misconfiguration; insecure APIs; network-slicing and edge exposure
7. Incident response and recovery engineering	Playbooks, tabletop exercises, tested backups, ransomware recovery, business continuity and public communication protocols.	Extended downtime; poor response coordination; reputational damage
8. Supply-chain and third-party assurance	Vendor risk scoring, contractual security requirements, software bill of materials, continuous monitoring and shared incident reporting.	Vendor compromise; concentration risk; opaque software dependencies

The framework should be implemented using measurable indicators. Suggested KPIs include percentage of critical assets covered by logging, percentage of privileged accounts protected by phishing-resistant MFA, mean time to detect, mean time to contain, ransomware recovery-test success rate, percentage of KEV-listed vulnerabilities remediated within policy timeframes, cloud configuration compliance, number of unresolved high-risk vendors and percentage of critical services with tested recovery plans.

VIII. PRACTICAL RECOMMENDATIONS

- Move from threat-label dashboards to service-impact dashboards. Every high-severity alert should be linked to affected critical services, crown-jewel data, privileged identities and service-continuity objectives.
- Prioritise Government-DDoS, telecommunications interception, IT-DDoS, IT-ransomware and banking web-application exposures as high-priority scenario families for tabletop exercises and control validation.

- Use CISA KEV, EPSS, CVSS, exploit intelligence and asset criticality together. Publicly exploited vulnerabilities on internet-exposed or operationally critical assets should override ordinary patch queues.
- Adopt zero-trust identity controls before expanding cloud, 5G and edge deployments. Identity is the control plane of distributed infrastructure.
- Develop AI-assisted detection but require explainability, governance and analyst oversight. Security automation must shorten response time without creating unreviewed operational changes.
- Test recovery, not just prevention. Critical-infrastructure cyber resilience should be measured by the ability to continue or restore essential services under ransomware, DDoS, cloud outage and vendor-compromise scenarios.
- Integrate cybersecurity into enterprise risk management and audit planning. This is consistent with the governance orientation of NIST CSF 2.0 and the broader risk-management literature.

IX. LIMITATIONS AND FUTURE RESEARCH

This study is limited by the structure of the public dataset. The dataset contains incident labels and impact indicators, but it does not include asset criticality, organisational size, control maturity, recovery costs, regulatory penalties, supply-chain dependency, cloud architecture, insurance coverage or verified incident narratives. The values should therefore be used for exploratory analytics and methodological demonstration rather than as a substitute for official breach statistics. Future studies should combine public incident data with vulnerability intelligence, CISA KEV records, asset inventories, EPSS probabilities, cloud posture metrics, identity logs and incident-response performance data. More advanced modelling could use graph neural networks, survival analysis for incident-resolution time, and causal inference to estimate the effect of specific controls such as MFA, segmentation, immutable backups and AI-assisted detection.

X. CONCLUSION

Critical-infrastructure cybersecurity is a national and economic resilience challenge. The empirical analysis in this paper shows that broad incident labels are useful but insufficient. DDoS, phishing, ransomware, SQL injection, malware and man-in-the-middle attacks all matter, yet their strategic significance depends on the sector, affected service, asset criticality, number of users exposed and time required to restore operations. The absence of strong statistical relationships between basic categorical labels and financial loss supports a more mature governance approach: organisations must integrate threat intelligence with asset context, vulnerability prioritisation, identity controls, cloud and 5G hardening, AI-assisted detection, incident response and recovery engineering. The proposed CICRF offers a practical framework for turning cyber incident analytics into board-level decisions and operational cyber resilience. In environments where public services, communications, finance, healthcare and infrastructure increasingly depend on cloud-connected and 5G-enabled systems, cybersecurity must be treated as a core component of national resilience, enterprise risk management and public trust.

Declarations

Data availability: The analytical dataset is publicly available through the Kaggle listing titled Global Cybersecurity Threats (2015-2024) and a public GitHub mirror. The manuscript uses aggregate outputs and visualisations generated from the downloaded CSV file.

Conflict of interest: None declared in this draft manuscript.

Ethics statement: The study uses publicly available, non-human-subject incident data and does not process personal identifiable information beyond aggregate affected-user counts already present in the dataset.

REFERENCES

[1] Aror, T.A. and Mupa, M.N. (2025) "Risk and compliance paper: What role does Artificial Intelligence (AI) play in enhancing risk management practices in corporations?", World Journal of Advanced Research and Reviews, 27(1), pp. 1072-1080. doi: 10.30574/wjarr.2025.27.1.2607.

[2] Barakabitze, A.A., Ahmad, A., Mijumbi, R. and Hines, A. (2020) "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges", Computer Networks, 167, 106984.

[3] CyberSeek (2025) Cybersecurity Supply and Demand Heat Map. Available at: https://www.cyberseek.org/heatmap.html (Accessed: 18 June 2026).

[4] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T.R. and Liyanage, M. (2024) "A survey on network slicing security: Attacks, challenges, solutions and research directions", IEEE Communications Surveys & Tutorials, 26(1), pp. 534-570. doi: 10.1109/COMST.2023.3312349.

[5] ENISA (2024) ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/ (Accessed: 18 June 2026).

[6] Ferrag, M.A., Maglaras, L., Janicke, H. and Smith, R. (2017) "Deep learning techniques for cyber security intrusion detection: A detailed analysis", in Proceedings of the 6th International Symposium for ICS & SCADA Cyber Security Research.

[7] GAO (2023) Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods, GAO-23-105468. Washington, DC: U.S. Government Accountability Office.

[8] Humayed, A., Lin, J., Li, F. and Luo, B. (2017) "Cyber-physical systems security - A survey", IEEE Internet of Things Journal, 4(6), pp. 1802-1831. doi: 10.1109/JIOT.2017.2703172.

[9] IBM (2025) Cost of a Data Breach Report 2025. IBM Security and Ponemon Institute. Available at: https://www.ibm.com/reports/data-breach (Accessed: 18 June 2026).

[10] Kaggle (2025) Global Cybersecurity Threats (2015-2024). Available at: https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024 (Accessed: 18 June 2026).

[11] Khan, R., Kumar, P., Jayakody, D.N.K. and Liyanage, M. (2020) "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions", IEEE Communications Surveys & Tutorials, 22(1), pp. 196-248. doi: 10.1109/COMST.2019.2933899.

[12] Maglaras, L., Janicke, H. and Ferrag, M.A. (2022) "Cybersecurity of critical infrastructures: Challenges and solutions", Sensors, 22(14), 5105. doi: 10.3390/s22145105.

[13] Moyo, T.M., Zhuwankinyu, E.K. and Mupa, M.N. (2024) "Leveraging Generative AI for an ethical and adaptive cybersecurity framework in enterprise environments", Iconic Research and Engineering Journals, 8(6), pp. 654-664.

[14] Nankya, M., Sam, A., Mkandawire, E. and Anagnostopoulos, M. (2023) "Securing industrial control systems: Components, cyber threats and machine learning-driven defence strategies", Sensors, 23, 8840.

[15] NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.CSWP.29.

[16] Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J.J., Lorca, J. and Folgueira, J. (2017) "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges", IEEE Communications Magazine, 55(5), pp. 80-87. doi: 10.1109/MCOM.2017.1600935.

[17] Ten, C.W., Manimaran, G. and Liu, C.C. (2010) "Cybersecurity for critical infrastructures: Attack and defense modeling", IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 40(4), pp. 853-865. doi: 10.1109/TSMCA.2010.2048028.

[18] Verizon (2024) 2024 Data Breach Investigations Report. Verizon Business. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 18 June 2026).

[19] Yigit, Y., Ferrag, M.A., Sarker, I.H., Maglaras, L.A., Chrysoulas, C., Moradpoor, N. and Janicke, H. (2024) "Critical infrastructure protection: Generative AI, challenges, and opportunities", arXiv preprint arXiv:2405.04874.

[20] Zhuwankinyu, E.K., Mupa, M.N. and Tafirenyika, S. (2025) "Graph-based security models for AI-driven data storage: A novel approach to protecting classified documents", World Journal of Advanced Research and Reviews, 26(2), pp. 1108-1124. doi: 10.30574/wjarr.2025.26.2.1631.