The State of Cybersecurity Awareness: An Interdisciplinary Analysis of Technical, and Policy Dimensions.

Priti Mule
Aarti Natekar
Dr. Rupali Kalekar
Dr. B. J. Mohite

Abstract

The world is witnessing a significant rise in cybersecurity incidents driven by increasingly sophisticated threats, rapid growth in digital connectivity, and persistent human vulnerabilities. Although advanced security technologies are being developed and many nations and international organizations continue to establish cybersecurity frameworks, a considerable gap remains between cybersecurity awareness and the actual secure behaviors practiced by users. This paper examines the state of cybersecurity awareness through three interconnected dimensions: human, technical, and policy.

The study identifies key human factors - such as susceptibility to social engineering, poor cyber hygiene practices, limited security knowledge, and weak organizational security culture - as major contributors to cybersecurity risks. It further analyzes the technical aspects of cybersecurity, highlighting common attack vectors, shortcomings in digital infrastructure, and the growing need for resilient and adaptive security architectures capable of addressing evolving threat landscapes. At the policy level, the research evaluates national cybersecurity strategies, compliance frameworks, regulatory guidelines, and awareness initiatives that aim to strengthen digital resilience.

Keywords: Cybersecurity Awareness, Human Factors, Cyber Hygiene, Social Engineering, Technical Vulnerabilities, Cyber Threats, Security Infrastructure, National Cybersecurity Strategies, Cyber Policies, Cyber Resilience, Data Breaches, Risk Management, Security Training, Cybersecurity Culture, Digital Safety.

Introduction

In the current digital age, cybersecurity has become critically important for individuals, organizations, and nation-states alike. The global adoption of digital technologies has brought immense convenience and efficiency, but it has also introduced major vulnerabilities within the digital ecosystem. Cybercrimes such as phishing, ransomware attacks, data breaches, and identity theft are increasing at an alarming rate, affecting millions of users every year. These rising threats necessitate immediate action and the strengthening of cybersecurity capabilities across all levels of society. While awareness of cyber threats is essential, it must be accompanied by the adoption of secure practices, responsible behavior, and effective policies to create a safer digital environment.

Among all elements of cybersecurity, the human factor has long been recognized as the most significant vulnerability. Even the most sophisticated technical defenses cannot fully protect against breaches caused by human errors, such as clicking malicious links, sharing passwords, or neglecting software updates. Many users remain unaware of how their everyday online behavior exposes them to cybersecurity risks. This gap between knowledge and actual practice creates an ideal environment for cyber attackers to exploit. Therefore, building a strong cybersecurity culture requires more than technological solutions—it demands continuous education, a shift in user attitudes, and the widespread adoption of safe digital habits. Enhancing human awareness is a crucial first step in reducing overall cyber risk and strengthening digital resilience. The challenge viewed from a technical perspective becomes more complicated, indeed. Organizations are situated in environments that consist of interlinked systems, cloud services, mobile devices, and IoT gadgets. The productivity of these systems is increased but so is the availability for cyberattacks. Technical flaws like poor network settings, unpatched software,

DOI: 10.55041/IJSREM54558

inadequate encryption, or no monitoring at all provide gateways for attackers to access systems almost effortlessly. The likes of firewalls, intrusion detection systems, and other high-tech tools can be utilized to decipher or diminish the dangers skillfully, but the effectiveness of these tools and measures heavily relies on proper application, routine upkeep, and expert personnel. Security measures alone, without the support of systematic technical awareness and readiness, cannot provide any protection, thus, their effectiveness will be limited.

Problem Statement

The rapid growth of digital technologies, cloud computing, mobile connectivity, and interconnected systems has transformed modern life but also expanded the attack surface for increasingly sophisticated cyber threats. Despite frequent guidelines issued by governments and cybersecurity agencies, a significant portion of the population remains unaware of how these threats affect their daily digital activities, making them vulnerable to phishing, ransomware, identity fraud, and social engineering. Since many attacks exploit human behavior rather than technical flaws, the human factor continues to be the weakest link in cybersecurity.

At the organizational level, outdated systems, weak security configurations, and limited monitoring further intensify risks. Although advanced security technologies exist, many institutions - especially small businesses and public sector organizations - lack the resources, trained staff, or structured processes to implement them effectively. This gap between available technology and actual implementation results in persistent technical vulnerabilities.

Policy frameworks and national cybersecurity strategies have been introduced worldwide, yet their impact is often limited by inconsistent enforcement, unclear communication, and difficulty in interpretation. Variations in regulations across regions further weaken coordinated efforts.

Literature Review

Cybersecurity has emerged as a critical domain of research due to the rapid digitalization of society, the growth of interconnected systems, and the escalating complexity of cyber threats. Existing scholarly work consistently highlights that effective cybersecurity requires a holistic understanding of human, technical, and policy factors. This literature review examines each of these dimensions to establish the foundations for analyzing the state of cybersecurity awareness.

---

1. Human Dimension of Cybersecurity Awareness

A large body of literature identifies the human factor as the most vulnerable element in cybersecurity defense. Studies consistently show that users often underestimate their exposure to cyber risks and lack adequate knowledge to navigate online threats. Research on social engineering indicates that attackers exploit psychological weaknesses rather than technical flaws, making phishing, impersonation, and manipulation among the most successful attack methods. It also highlighted poor cyber hygiene practices such as weak passwords, reuse of credentials, ignoring security warnings, and failing to update software as major contributors to breaches.

Organizational studies emphasize that security culture plays a central role in shaping employee behavior. Organizations with strong cybersecurity culture, regular training, and awareness programs report significantly lower incident rates compared to those that rely solely on technical tools. The literature suggests that cybersecurity awareness programs must be continuous, practical, and behavior-focused to effectively reduce human-related vulnerabilities.

2. Technical Dimension: Infrastructure, Vulnerabilities, and Defenses

Technical literature underscores the growing complexity of digital ecosystems that include cloud platforms, IoT devices, mobile networks, and distributed systems. As these technologies evolve, they introduce new vulnerabilities that cybercriminals exploit. Researchers have noted that misconfigured networks, outdated software, weak encryption, and insufficient monitoring are among the most common technical weaknesses.

Advanced defensive systems such as firewalls, intrusion detection and prevention systems, endpoint protection, and AI-driven threat analytics have become central to modern cybersecurity strategies. However, studies emphasize that these tools are only effective when implemented correctly, updated regularly, and supported by skilled personnel. The gap between the availability of advanced tools and the capability of organizations to deploy them effectively is a recurring theme in the literature.

Furthermore, research on IoT security highlights that low-cost devices often lack robust security features, dramatically increasing the attack surface. Similarly, cloud security literature stresses shared responsibility models, which many organizations still misunderstand, leading to avoidable vulnerabilities.

3. Policy Dimension: Regulations, Frameworks, and Compliance

From a policy standpoint, significant research has examined the role of national cybersecurity strategies, international standards, and organizational governance frameworks. Global initiatives such as cybersecurity frameworks, privacy regulations, and data protection laws aim to strengthen digital resilience and ensure consistent security practices.

However, the literature indicates that policy effectiveness varies widely across regions and industries. Key challenges include inconsistent enforcement, lack of organizational compliance, limited resources, and difficulties interpreting complex regulations. Scholars argue that policies often fail to reach the general population due to communication gaps and limited public awareness.

Research further suggests that policies alone cannot drive secure behavior unless supported by cultural change, leadership involvement, and accessible awareness programs. The misalignment between policy intentions and actual practice remains a significant barrier to building broad cybersecurity awareness.

Summary

The reviewed literature highlights three recurring themes:

1. Humans remain the most exploited vulnerability, requiring continuous education and behavioral change.

2. Technical systems are increasingly complex, and their security depends on skilled implementation and regular maintenance.

3. Policies exist but are often poorly enforced or understood, limiting their effectiveness in improving security awareness.

Research Methodology

This study adopts a mixed-methods, interdisciplinary research design integrating technical analysis, human-behavior assessment, and policy evaluation. The methodology is structured into four major components: data collection, data analysis, evaluation framework, and validation.

Research Design

A descriptive and analytical research design was used to understand cybersecurity awareness from three perspectives:

1. Technical Dimension:
Examining threat trends, system vulnerabilities, and the effectiveness of security tools.
2. Human and Behavioral Dimension:
Assessing user awareness, risk perception, digital behavior, and susceptibility to cyber threats.

3. Policy and Governance Dimension:
Analyzing cybersecurity regulations, institutional frameworks, and organizational policies.

This interdisciplinary design helps identify connections between human actions, technology use, and policy enforcement.

Data Collection Methods

Secondary Data Collection

Secondary sources were extensively used to build a theoretical foundation and identify existing research gaps:

- Academic journals (IEEE, ACM, Springer)
- Cybersecurity reports (IBM, Cisco, Verizon DBIR)
- Government and regulatory documents (CERT-In, NIST, GDPR)
- Policy frameworks and awareness guidelines

These sources provided insights into global cyberattack trends, user awareness levels, and policy implementations.

Data Analysis Techniques

Technical Analysis

Security reports were analyzed to identify:

- The most common attack vectors
- Frequency and severity of cyber incidents
- Human-error contributions to cyber breaches
- Effectiveness of security tools (authentication, encryption, endpoint protection)

Trend analysis was applied to detect yearly changes in cybersecurity incidents.

Behavioral Analysis

Collected data was analyzed using:

- Descriptive statistics: percentages, mean scores, response distributions

- Risk-awareness scoring: identifying high-risk behavior (weak passwords, link-clicking habits)

Qualitative responses were thematically analyzed to understand perceptions and attitudes.

Policy Analysis

Policy documents and organizational frameworks were examined using:

- Comparative analysis: comparing Indian, U.S., and EU cybersecurity policies

- Content analysis: identifying strengths, weaknesses, and enforcement challenges

- Gap analysis: comparing existing policies with real-world user behaviors and technological needs

---

Evaluation Framework

The study applies a tri-layer cybersecurity awareness evaluation framework:

1. Technical Readiness – Tools, defenses, and infrastructure.

2. Human Awareness – Skills, training, decision-making behavior.

3. Policy Strength – Regulatory support, implementation, and compliance.

This framework enables a holistic understanding of cybersecurity maturity.

Result and discussion

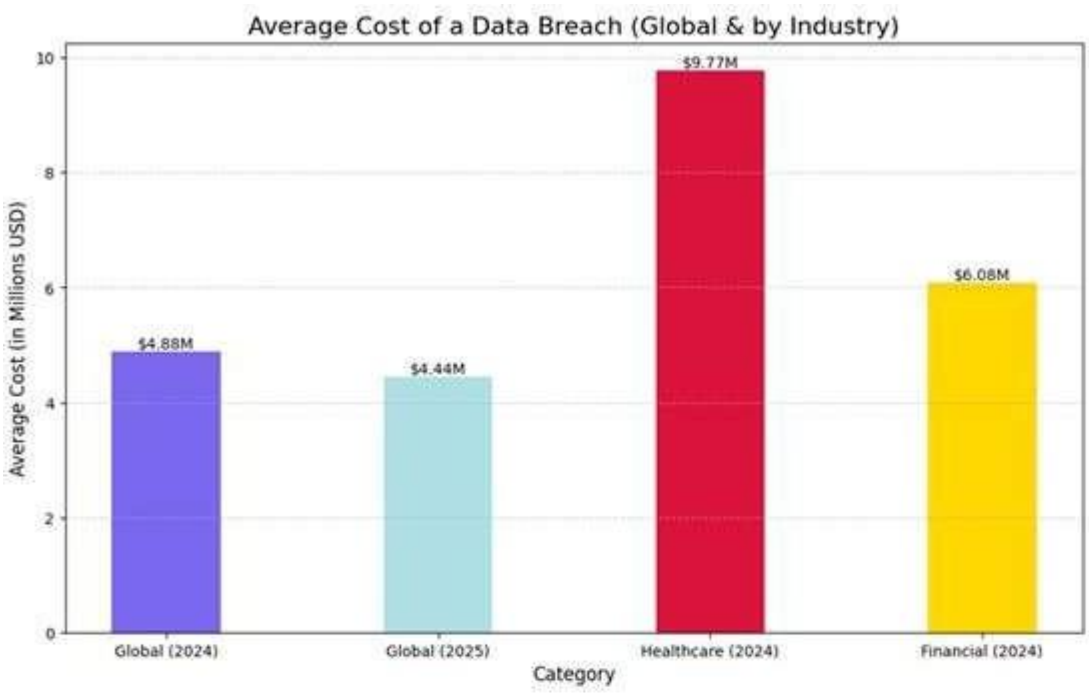
The global escalation of cybercrime continues on an explosive trajectory, both in scale and financial impact. Yet, a deeper examination of current data reveals a striking strategic contradiction in how organizations are responding to this surge. While cyber threats intensify, corporate strategies increasingly prioritize technological investments over human-centric security measures—despite overwhelming evidence that human behavior remains the most exploited vulnerability.

Financial and Reputational Impact of Cybercrime

Cybercrime imposes a massive and steadily growing economic burden. In 2024, the average global cost of a data breach reached $4.88 million, marking a 10% increase from the previous year and the most significant spike since the pandemic. Although the average decreased slightly to $4.44 million in 2025, this still represents the second-highest breach cost ever recorded, demonstrating the long-term upward trend.

The financial impact is not uniform across industries. For the 14th consecutive year, the healthcare sector reported the most expensive breaches, averaging $9.77 million in 2024, followed closely by the financial sector, which recorded an average cost of $6.08 million per breach—both well above the global average.

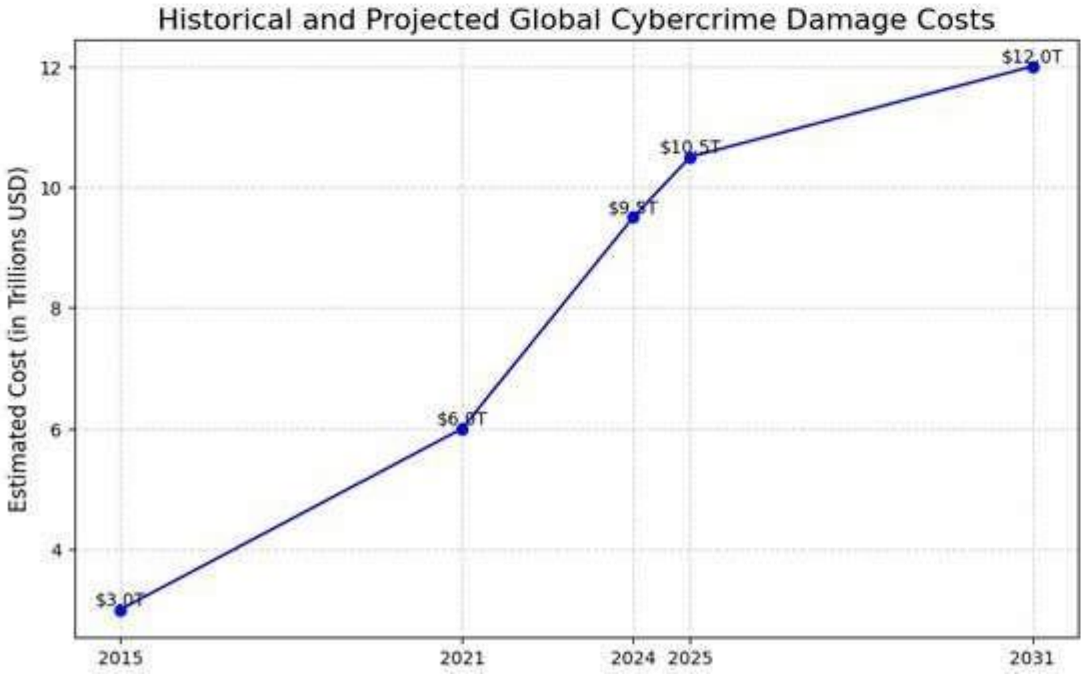
Beyond direct financial losses, data breaches also inflict severe reputational damage, eroding customer trust, weakening brand credibility, and decreasing market competitiveness. These intangible losses often exceed the measurable financial impact, making cyber incidents not only operational challenges but existential threats to organizational stability.



Statistical Trajectory of Cybercrime and Rising Breach Costs

A longitudinal analysis of global cybercrime data indicates that cyberattacks are increasing not only in number but in sophistication and potential damage. The rise is exponential rather than linear, reflecting expanding digital infrastructures, increased data mobility, interconnected systems, and a globally distributed online workforce.

Historical and Projected Global Cybercrime Damage Costs:



The accelerated growth of cybercrime underscores the urgency for more effective cybersecurity strategies. However, current organizational responses reveal a critical strategic disconnect.

Despite 85% of organizations increasing their cybersecurity budgets in 2024, investment in employee security skill development has declined from 58% to 51% over recent years. This shift illustrates a significant misalignment: companies are allocating more resources to advanced security technologies, while underinvesting in the human element, which remains the primary gateway for cyber threats.

This imbalance exposes a systemic misconception—attempting to solve a behavioral vulnerability (human error) with technological solutions alone. As a result, organizations unintentionally leave major security gaps unaddressed, perpetuating a cycle in which cyberattacks continue to succeed despite increased financial spending on tools and systems

Findings and Suggestions

Findings

Based on the interdisciplinary analysis across human, technical, and policy domains, several key findings emerge:

1. Human behavior remains the primary vulnerability

Despite technological advancements, most cyberattacks still exploit human error, including falling for phishing emails, social engineering, weak passwords, and unsafe browsing behavior. A significant portion of users remain unaware of modern attack techniques, demonstrating that awareness does not translate into secure behavior.

2. Technology investments are increasing, but not effectively utilized

Organizations have increased cybersecurity budgets, yet many still operate with:

- outdated systems,
- unpatched software,
- poorly configured networks, and
- lack of continuous monitoring.

3. Policies exist, but enforcement and comprehension are weak

Governments and organizations have introduced cybersecurity frameworks, standards, and awareness campaigns. However:

- enforcement is inconsistent,
- guidelines are often difficult to interpret,
- organizations lack resources to comply fully, and
- awareness campaigns fail to reach a broad audience.

This creates a gap between policy intent and actual practice, reducing the impact of regulatory measures.

4. Fragmentation across domains widens the awareness gap

There is little coordination between the human, technical, and policy dimensions. For example:

- policies are created without considering individual user behavior,
- organizations deploy tools without corresponding human training,
- users receive general awareness messages that do not align with actual organizational security practices.

This lack of integration causes inconsistencies and leads to persistent vulnerabilities.

5. Cybercrime is rising faster than cybersecurity maturity

Statistical evidence shows exponential growth in cybercrime cost and sophistication. Yet cybersecurity maturity—especially in smaller organizations—grows at a much slower pace. The imbalance increases global exposure to digital threats.

Suggestions

Based on the findings, the following recommendations are proposed to strengthen cybersecurity awareness and resilience across all levels:

1. Prioritize continuous cybersecurity training

Cybersecurity training should shift from one-time sessions to continuous, adaptive learning. Organizations should implement:

- periodic phishing simulations,
- real-time behavioral feedback,
- scenario-based training for emerging threats, and
- awareness programs tailored to different user groups.

This will reduce human error and promote secure digital habits.

2. Strengthen technological readiness and routine monitoring

Organizations must ensure that security tools are not only purchased but properly implemented. This includes:

- enforcing regular patch management,
- conducting system audits,
- improving network configurations,
- upgrading outdated infrastructure, and
- hiring or training skilled cybersecurity personnel.

Technology must be supported by expert oversight and timely updates.

3. Improve policy enforcement, clarity, and accessibility

Policymakers should:

- simplify cybersecurity frameworks,
- provide clearer compliance guidelines,
- ensure nationwide enforcement,
- support small organizations with subsidized cybersecurity programs, and

- improve public awareness campaigns through targeted communication channels.

Clearer and more enforceable policies will lead to better cybersecurity adoption.

4. Adopt an integrated cybersecurity model

A holistic approach is essential. Organizations should align:

- technical safeguards,
- human behavior programs, and
- policy compliance initiatives.

This integrated model ensures that each dimension strengthens the others, creating a more resilient cybersecurity environment.

5. Foster a culture of shared responsibility

Cybersecurity should not be seen as solely an IT issue. It requires participation from:

- employees,
- management,
- policymakers,
- vendors,
- and the general public.

Promoting a culture where everyone plays an active role will reduce vulnerabilities and enhance overall digital resilience.

References

- (ISC)². (2020). Cybersecurity Perception Study. Retrieved from https://alltogether.swe.org/2021/10/4-barriers-to-diversity-in-cybersecurity-and-how-to-address-them/
- Accenture. Cyber Resilience report. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- ArcticWolf. Report on business email compromise. Retrieved from https://www.cobalt.io/blog/top-cybersecurity-statistics-2025
- Belfer Center for Science and International Affairs. (n.d.). Cybersecurity Strategy Scorecard. Retrieved from https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard
- Business Research Insight. (n.d.). Global cybersecurity market report. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- Chainalysis. (n.d.). Ransomware cryptocurrency heists data. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

- CISA. (n.d.). CISA Cybersecurity Awareness Program. Retrieved from https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program
- CISA. (n.d.). Cybersecurity Awareness Month Toolkit. Retrieved from https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-month-toolkit
- Cloudflare. (n.d.). Phishing attack. Retrieved from https://www.cloudflare.com/learning/access-management/phishing-attack/
- Comcast Business. (n.d.). Cybersecurity Threat report. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- Committee on Publication Ethics (COPE). (1999). Plagiarism definition. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC4212376/
- CrowdStrike. (n.d.). Cyberattacks. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/
- Dataguard. (n.d.). Cyber Security Awareness. Retrieved from https://www.dataguard.com/cyber-security/awareness/
- DHS. (n.d.). Cybersecurity. Retrieved from https://www.dhs.gov/topics/cybersecurity
- EDUCAUSE. (n.d.). Cybersecurity Program Awareness Campaigns. Retrieved from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns
- European Commission. (n.d.). EU Cybersecurity Strategy. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
- European Union Agency for Cybersecurity (ENISA). (n.d.). CyberSecMonth. Retrieved from https://cybersecuritymonth.eu/about-ecsm
- F5. (n.d.). Cybersecurity Glossary. Retrieved from https://www.f5.com/glossary/cybersecurity
- Federal Bureau of Investigation (FBI). (n.d.). Internet Crime Complaint Center (IC3) report. Retrieved from https://www.cobalt.io/blog/top-cybersecurity-statistics-2025
- Fortinet. (n.d.). Cybersecurity Statistics. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- Fortra. (n.d.). State of Cybersecurity Survey Results. Retrieved from https://www.fortra.com/resources/guides/fortra-state-cybersecurity-survey-results
- Hempstead, N.Y. (n.d.). Famous Phishing Incidents from History. Retrieved from https://www.hempsteadny.gov/635/Famous-Phishing-Incidents-from-History
- Hiscox. (2024). Hiscox Cyber Readiness Report 2024. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- IBM. (2024). Cost of a Data Breach Report 2024. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- IBM. (n.d.). Cybersecurity Trends. Retrieved from https://www.ibm.com/think/topics/cybersecurity
- Infosec IQ. (n.d.). Cybersecurity Culture Survey. Retrieved from https://www.infosecinstitute.com/iq/reporting/cybersecurity-culture-survey/
- Javelin Strategy & Research. (2025). 2025 Identity Fraud Study. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- Kyndryl. (2024). 5 cyber education program mistakes. Retrieved from https://www.kyndryl.com/us/en/about-us/news/2024/10/5-cyber-education-program-mistakes
- Mass.gov. (n.d.). Types of Cyber Threats. Retrieved from https://www.mass.gov/info-details/know-the-types-of-cyber-threats
- Network for Public Health Law. (n.d.). Cybersecurity Awareness Month Resources. Retrieved from https://www.networkforphl.org/news-insights/cybersecurity-awareness-month-resources-for-covered-entities/
- NIS 2 Directive. (n.d.). What is the NIS 2 Directive?. Retrieved from https://www.nis-2-directive.com/
- NSA. (n.d.). Cybersecurity. Retrieved from https://www.nsa.gov/cybersecurity/

- Paubox. (n.d.). Negligence in Cybersecurity. Retrieved from https://www.paubox.com/blog/negligence-in-cybersecurity
- Proofpoint. (n.d.). Security Awareness Training. Retrieved from https://www.proofpoint.com/us/threat-reference/security-awareness-training
- Proofpoint. (n.d.). NIS2 Directive. Retrieved from https://www.proofpoint.com/us/threat-reference/nis2-directive
- PwC. (2024). 2024 Global Digital Trust Insights. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- ResearchGate. (2018). The knowledge-behavior gap. Retrieved from https://www.cscan.org/openaccess/?id=393
- ResearchGate. (2021). Comparative Analysis of National Cyber Security Strategies. Retrieved from https://www.researchgate.net/publication/357457984_Comparative_Analysis_of_National_Cyber_Security_Strategies_using_Topic_Modelling
- ResearchGate. (2024). Bridging the Gaps: Evaluating Cybersecurity Awareness and Practices. Retrieved from https://www.researchgate.net/publication/391500663_BRIDGING_THE_GAPS_EVALUATING_CYBERSECURITY_AWARENESS_AND_PRACTICES_FOR_ENHANCED_DIGITAL_SECURITY
- ResearchGate. (n.d.). From Awareness to Action: Designing effective cybersecurity training programs. Retrieved from https://www.researchgate.net/publication/395093125_From_Awareness_to_Action_Designing_effective_cybersecurity_training_programs
- ResearchGate. (n.d.). Influence of Awareness and Training on Cyber Security. Retrieved from https://www.researchgate.net/publication/240236007_Influence_of_Awareness_and_Training_on_Cyber_Security
- SentinelOne. (n.d.). Vulnerability Assessment Framework. Retrieved from https://www.sentinelone.com/cybersecurity-101/cybersecurity/vulnerability-assessment-framework/
- Sibermate. (2025). Psychology's role in raising cybersecurity awareness. Retrieved from https://sibermate.com/hrmi/blog/psychologys-role-in-raising-cybersecurity-awareness
- Splunk. (n.d.). Vulnerability vs. Threat vs. Risk. Retrieved from https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html
- Trent University. (n.d.). How to paraphrase and summarize. Retrieved from https://www.trentu.ca/academicskills/how-guides/how-use-sources/avoiding-plagiarism/paraphrasing-and-summarizing
- UpGuard. (n.d.). Biggest Data Breaches US. Retrieved from https://www.upguard.com/blog/biggest-data-breaches-us
- Verizon. (2024). 2024 Verizon DBIR report. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- World Economic Forum. (2024). Global Risks Report 2024. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
- World Economic Forum. (2025). Global Cybersecurity Outlook Report 2025. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics