Basics Of Cyber Security and Threat Prevention

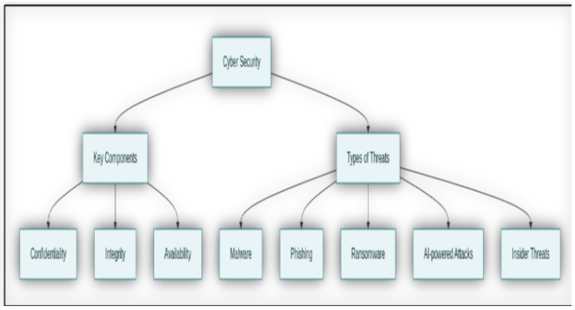
Avdhoot Ajay Tambat[1]. Vivek Sanjeev Keertiwar[2], Sameer Husen Attar[3]

***Abstract*—Cyber security is a crucial field focused on protecting digital systems, networks, and sensitive data from an array of malicious threats and attacks that continue to increase in frequency and sophistication in the modern technological era. These threats range from malware and ransom ware to phishing, denial-of-service attacks, and data breaches, posing significant risks to individuals, corporations, and national infrastructure.**

"Global Data Breaches and Cyber Attacks in August 2025" by IT Governance Analysts, published on September 7, 2025, from the bibliography point no. 8, analyzes the surge in data breaches during the month, with over 17.3 million records exposed across at least 30 major incidents. The report identifies sectors such as telecom, healthcare, and cloud services as primary targets, with significant breaches involving Bouygues Telecom and Salesforce-linked partners. Attackers used diverse techniques, including ransom ware, O-Auth token theft, and exploiting cloud or software vulnerabilities, to access sensitive personal and corporate data. The findings point to growing threats facing SaaS and CRM platforms, as well as the persistent dangers from supply-chain and third-party vulnerabilities. The study underscores the urgent need for proactive cyber security practices and continuous vulnerability assessment to combat increasingly sophisticated attacks.

I. INTRODUCTION

Cyber security has become a critical field as digital transformation accelerates across all sectors worldwide. The global cyber security market is projected to reach approximately USD 272 billion by 2025 and continue its rapid growth due to increasing cyber threats, such as data breaches, ransom ware, and AI-enhanced attacks. The rise of cloud computing, IOT devices, remote work, and digital services expands the attack surface, making organizations more vulnerable to cyber incidents. Consequently, businesses and governments are investing heavily in advanced cyber security solutions that include threat detection, prevention, and response techniques to safeguard sensitive data and maintain trust in digital ecosystems. Emerging technologies like AI and machine learning are playing a vital role in evolving these defenses to meet continuously sophisticated cyber threats.



The purpose of this research on cyber security and threats is to analyze the evolving landscape of cyber-attacks and the development of modern security systems aimed at mitigating these risks. Significant advancements include the launch of the Global Cyber security Resilience Center in January 2024, designed to enhance threat intelligence sharing and coordinated response. In July 2024, Japan introduced its Cyber Defense Framework 2.0, incorporating AI-powered threat detection.

II. LITERATURE REVIEW

Cyber security has evolved into a critical component of modern digital life, encompassing the protection of information systems, networks, and data from unauthorized access, attacks, and damage. According to Goel (2019), cyber security includes a broad range of strategies, technologies, policies, and human factors aimed at safeguarding the cyber environment, including systems, networks, and user assets.

Date	Research Paper Name	Authors	Description
2025	Cyber Security and Applications	Dr. Rajendra Pamula	Focuses on cyber security applications, vulnerabilities, and mitigation techniques.
Sep 26, 2025	Security Week Cyber Insights 2025	Mike Lennon	Discusses cyber security regulations and emerging trends for 2025.
Sep 25, 2025	SANS Cyber Security Research Papers	Stephen Northcutt	Covers latest advances in incident response, threat hunting, and cloud security.
Sep 25, 2025	NIST Cryptographic Module Validation Automation	Dr. Matthew Scholl	Explores automation and standards for validating cryptographic modules.
Sep 24, 2025	Journal of Cyber Security	Dr. Mohammed Anbar	Open-access publishing on technical and application security research.
Sep 16, 2025	Unit 42 Global Incident Response Report	Philippa Cogswell	Examines rapidly evolving multi-vector cyber-attacks and AI-driven phishing.
Sep 8, 2025	Hornet Security Monthly Threat Report	Daniel Hofmann	Highlights AI privacy concerns, SaaS vulnerabilities, and connector exploits.
Sep 7, 2025	Global Data Breaches August 2025 (IT Governance)	Luke Irwin	Details recent major data breaches, records exposed, and attack methods.
Aug 29, 2025	The Hacker News Threats Day Bulletin	Mohit Kumar	Provides weekly cyber news, threat intelligence, and practical attack updates.
Aug 7, 2025	Top Cyber Security Threats in 2025 (USD)	Dr. Michelle Moore	Reviews AI-powered risks, deep fakes, and evolving malware threats.
Jun 24, 2025	ENISA Threat Intelligence Publications	Juhan Lepassaar	Focuses on EU cyber threat intelligence, regulation, and resilience.
May 27, 2025	Wipro State of Cyber Security Report 2025	Rohit Adlakha	Analyzes AI in threat detection, cost optimization, and CISO priorities.
May 22, 2025	Cyber Security Case Studies 2025 (EIMT)	Prof. Daniel Gomes	Presents major global cyber security case studies and lessons learned.
Feb 26, 2025	Crowd Strike 2025 Global Threat Report	Adam Meyers	Offers global threat analysis and cyber security incident statistics.

Date	Research Paper Name	Authors	Description
Jan 26, 2025	Global Cyber Security Outlook 2025 (WEF)	Prof. Dr. Alina Matyukhina	Addresses international cooperation, trends, and supply chain challenges.
Jan 13, 2025	Checkpoint Cyber Security Report 2025	Maya Horowitz	Reviews attack trends, threat types, and mitigation priorities.
Jan 1, 2025	Cyber Defense Magazine	Gary S. Miliefsky	Provides daily cyber security news and defense analysis.
Dec 31, 2024	Oxford Academic Journal of Cyber Security	Tyler Moore, David Pym	Publishes peer-reviewed interdisciplinary cyber security research.
Sep 30, 2023	Journal of Cyber Security Technology (Taylor & Francis)	Dr. Hani Muheidat	Covers new technologies and application security research.
Dec 31, 2023	Slogix Journals of Cyber Security	Dr. S. Smys	Lists indexed journals and open cyber security research resources.

III. OBJECTIVES

A. Analyze the latest cyber security threats, attack vectors, and vulnerabilities: Research on evolving threats, including AI-powered risks, phishing techniques, SaaS vulnerabilities, multi-vector attacks from Unit 42, Hornet Security, and Crowd Strike reports.

AI-driven monitoring and behavior analysis
Deep fake
Phishing
Ransomware
detect and counter emerging threats

B. Evaluate cyber security mitigation strategies, detection techniques, and incident response frameworks: Understanding mitigation and response from NIST standards, SANS incident response research, Checkpoint and Wipro defense reports.

Continuous Learning of Attacker Patterns
Predictive Threat Detection
Autonomous System Response

C. Investigate the impact and trends of emerging technologies on cyber security, including AI, cloud, and cryptographic automation: Studies on AI threat detection, cryptographic module validation automation, cloud security from SANS and NIST sources.

D. Examine global cyber security regulations, compliance standards, and cooperation initiatives: Analysis of ENISA publications, WEF global outlook, Security Week regulatory trends, and IT Governance breach reports.

Compliant Cybersecurity Defenses
Network Access Control
Continuous Authentication Privilege
Continuous Authentication Zeest
Least Immutable Ledger
Blockchain Tamper Resistance

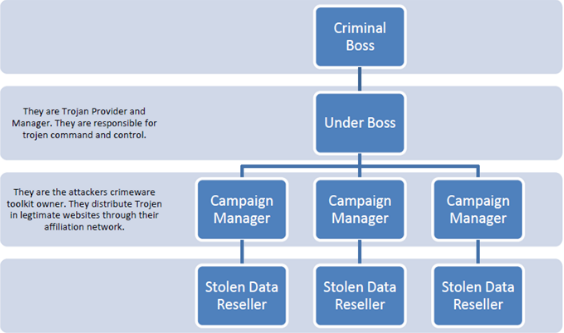
E. Conduct case studies on major cyber security breaches and lessons learned for improving defenses: Compilation and review of global case studies from EIMT, IT Governance breach datasets, and Hacker News threat bulletins.

Cybersecurity Breaches & Defensive Lessons
password
Strengthening Defenses Through Experience

IV. JUSTIFICATION AND IMPORTANCE OF FURTHER RESEARCH

- The frequency and impact of cyber-attacks continue to increase—global cyber-crime costs are projected to reach $10.5 trillion annually in 2025, while the average cost of a data breach is $4.88 million. This highlights a growing necessity for new prevention and response strategies.
- Emerging technologies such as artificial intelligence, quantum computing, and deep fake tools create both new opportunities and uncharted risks. Research supports understanding these dangers and developing effective countermeasures.
- The interconnectedness of modern systems means vulnerabilities in supply chains, third-party platforms, and remote work arrangements can cascade into widespread disruptions; dedicated research is needed to anticipate and mitigate these complex risks.

5.1 Classification of Cyber Crimes:



They are Trojan Provider and Manager. They are responsible for trojen command and control.

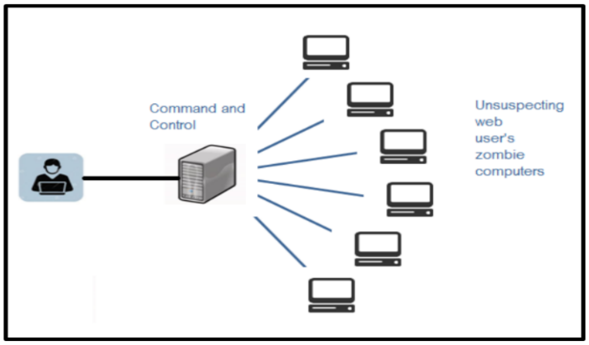
They are the attackers crimeware toolkit owner. They distribute Trojen in legtimate websites through their affiliation network.

Above figure shows the hierarchical structure of a cybercrime organization. At the top is the Criminal Boss, followed by the Under Boss, who acts as the Trojan provider and manager responsible for command and control. Below them are several Campaign Managers who handle the distribution of crime ware and launch attacks via affiliate networks. At the bottom are Stolen Data Resellers, who sell the stolen data obtained from cyber-attacks. The diagram highlights roles from leadership to data monetization within a cybercrime ecosystem.

1. Insider Attack: An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors.

2. External Attack: When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber-attack not only faces financial loss but also the loss of reputation.

5.2 Malware and It's Types:



Above figure depicts a classic example of a botnet attack in cyber security. A malicious actor uses a server for command and control, centrally managing the compromised system. The infected server sends commands out to multiple unsuspecting web users' computers, which have unknowingly turned into zombie machines. The diagram shows the hierarchical relationship where the attacker orchestrates all actions via the command server. It illustrates the risk to regular internet users whose devices may be hijacked without their knowledge.

Malware stands for "Malicious Software" and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. Malware spreads through vulnerabilities, infected downloads, phishing, or social engineering. Protection involves using antivirus software, firewalls, system updates, cautious browsing, and employee awareness. Hybrid malware combining multiple types is increasingly common, complicating defense efforts. Malware can steal sensitive information, disrupt operations, gain unauthorized access, or cause other harmful effects. Protection against malware involves using antivirus software, firewalls, regular software updates, and safe browsing practices. Some of the popular ones are:

a. Adware: It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event.

b. Spyware: It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine

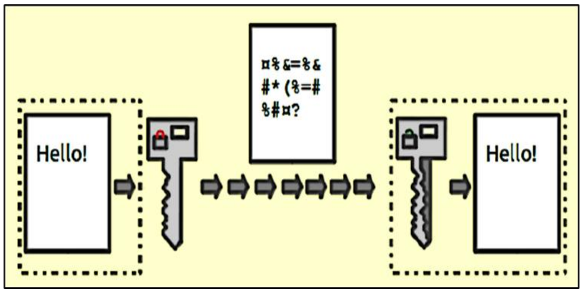
c. Browser hijacking software: There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user.

d. Virus: A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc.

e. Worms: They are a class of virus which can replicate themselves. They are different from the virus by the fact that they do not require human intervention to travel over the network and spread from the infected machine to the whole network.

f. Trojan horse: Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source.

5.3 Encryption:



It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

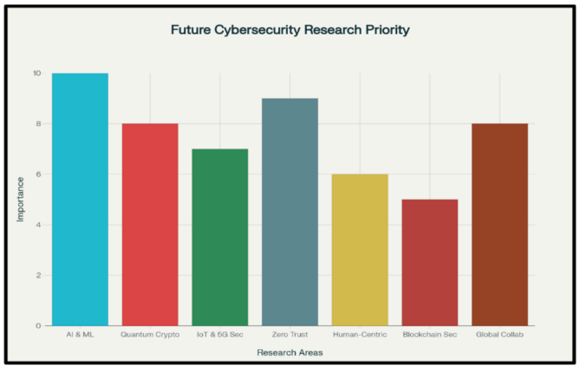
V. FUTURE SCOPE OF STUDY

- Development of advanced artificial intelligence and machine learning models for proactive threat detection, prediction, and autonomous response systems to reduce reaction time and human error.
- Research on quantum-resilient cryptography to prepare for the advent of quantum computing, which threatens to break existing encryption standards.
- Securing Internet of Things (IOT) ecosystems and smart infrastructure given their exponential growth, focusing on device authentication, data privacy, and secure communication protocols.
- Enhancement of zero trust security models and adaptive access controls tailored for decentralized, hybrid, and multi-cloud environments.
- Investigation of human factors in cyber security, including socio-technical approaches to improve user awareness, behavioral analytics, and insider threat mitigation.
- Exploration of block chain and distributed ledger technologies as tools to improve data integrity, transparency, and secure transactions.
- Strengthening international cooperation frameworks and policy research to tackle global cybercrime, improve intelligence sharing, and align regulatory standards.

VI. RESEARCH RESULTS

1. Cyber threats are constantly evolving with new types of attacks, including AI-powered threats and more complex multi-vector attacks that target networks and cloud systems.
2. Incident response and threat hunting methods are improving, helping organizations detect and respond to attacks faster, especially with automated tools and AI assisting in identifying threats.
3. Major data breaches continue to expose millions of sensitive records globally, often due to vulnerabilities in software or weak security practices. Learning from these breaches can help improve defenses.
4. Strong cyber security regulations and international cooperation are essential to handle the growing cyber risks across sectors, as seen in EU and global frameworks.
5. Automation and standards, such as cryptographic validations, play an important role in ensuring systems are secure and trusted.
6. Cyber security applications focus on identifying vulnerabilities in software and creating mitigation strategies to reduce risks, using new defense technologies and continuous monitoring.
7. Privacy concerns related to AI and SaaS environments continue to grow as attackers exploit cloud vulnerabilities.
8. Emerging technologies such as quantum computing and deep learning present both new challenges and opportunities for cyber security.
9. Awareness and continuous education on cyber security risks and best practices are vital to reduce human error, a major factor in cyber incidents.
10. The cyber security landscape's future depends heavily on integrating emerging technologies with traditional security methods to effectively counter complex and persistent threats

VII. FUTURE RESEARCH DIRECTIONS



Above figure presents the future priorities for cyber security research as perceived in 2025. AI & Machine Learning is marked as the top priority, underscoring the need to integrate intelligent threat detection and response systems. Zero Trust architecture follows closely, emphasizing the importance of strict access controls. Other significant areas include Quantum Cryptography and Global Collaboration, reflecting the need for advanced encryption and cooperative efforts across organizations. The graph also highlights a moderate focus on IOT & 5G security and human-centric approaches, indicating evolving challenges in connected devices and user behavior. Block chain security, while important, is ranked as a slightly lower priority within this forward-looking research agenda.

- AI and Machine Learning Advancements: Creating autonomous threat detection and response systems leveraging advanced AI to predict and counter zero-day exploits and sophisticated attack patterns more effectively.
- Quantum-Resistant Cryptography: Developing and standardizing encryption methods that withstand quantum computing-powered attacks to future-proof data security.
- IOT and 5G Security: Designing frameworks and protocols to secure exponentially growing IOT networks and 5G infrastructure from new vulnerabilities due to scale and connectivity.
- Zero Trust Security Models: Research into tailoring zero trust principles for hybrid and multi-cloud architectures, emphasizing continuous verification and least privilege access.
- Human-Centric Cyber security: Exploring socio-technical approaches addressing human errors, insider threats, and enhancing cyber security education and awareness.
- Block chain Security investigates ways to secure distributed ledgers used in finance, supply chains, and identity management.
- Global Collaboration highlights the importance of international cooperation against cyber threats and regulatory challenges.

VIII. LIMITATIONS

1. Rapidly Evolving Threat Landscape: Cyber threats, especially AI-driven attacks and deep fakes, evolve so quickly that research findings can become outdated rapidly, making it hard to maintain cutting-edge protective measures.
2. Talent Shortage: There is a persistent shortage of skilled cyber security professionals, with 83% of executives citing workforce limitations as a barrier to implementing effective security strategies. This limits the pace at which new research can be applied and disseminated.
3. Complexity of Emerging Technologies: New technologies like quantum computing and IOT bring complex vulnerabilities that existing research may only partially address, requiring multidisciplinary and highly specialized approaches.
4. Data Availability and Privacy: Conducting large-scale empirical research is often constrained by limited access to real-world attack data and privacy concerns, impeding comprehensive threat analysis.
5. Budget limitations: Often prevent organizations from implementing and maintaining robust security measures, especially for smaller businesses and budgets.
6. Human error and lack of security awareness: Among users continue to be exploited by social engineering and phishing attacks, leading to successful breaches.

IX. NATIONAL CONTEXT

A. Critical Infrastructure Protection: Nations invest in securing government, energy, finance, and healthcare systems from cyber-attacks, as breaches in these sectors can severely disrupt national stability, economy, and public welfare. Cyber security policies emphasize defending critical information infrastructure against evolving threat vectors with advanced defensive technologies and timely incident response mechanisms.

B. National Cyber security Governance and Coordination: Countries establish agencies and frameworks to coordinate cyber security efforts across government departments, private sector, and academia. For example, India's National Security Council Secretariat (NSCS) coordinates cyber strategy and exercises like Bharat NCX 2025 to simulate real-world attack scenarios, enhancing preparedness.

C. Cyber Crime and Legal Frameworks: National legislation is developed to combat cybercrime, enforce data protection, and regulate cyber security practices. These laws provide legal backing for prosecuting malicious actors and stipulating organizational responsibilities in cyber security, fostering a safer digital environment.

D. Capacity Building and Awareness: Nations focus on developing skilled cyber security workforce and enhancing public awareness. Training programs, certifications, and simulations aim to build technical expertise and promote responsible cyber hygiene among citizens and organizations.

E. Technology Adoption and Innovation: Countries promote research and adoption of emerging technologies such as AI, 5G, cloud computing, and quantum-resistant cryptography to enhance cyber defenses. National cyber security strategies integrate these technologies to address sophisticated and automated cyber threats in an increasingly digital society.

X. INTERNATIONAL CONTEXT

A. Cross-border Nature of Cyber Threats: Cyber-attacks are transnational, targeting entities globally and emphasizing the need for international cooperation to detect, mitigate, and investigate cyber incidents effectively across jurisdictions.

B. International Cyber security Norms and Agreements: Global bodies such as the UN, NATO, and the World Economic Forum promote norms for responsible state behavior in cyberspace, focusing on preventing cyber warfare escalation, protecting critical infrastructure, and fostering mutual trust among nations.

C. Information Sharing and Collaboration: Countries collaborate through international forums and alliances to share cyber threat intelligence, conduct joint cyber exercises, and coordinate responses. This cooperation strengthens global cyber resilience against emerging complex threats like ransom ware and state-sponsored attacks.

D. Regulatory Harmonization and Challenges: Diverse regulatory frameworks worldwide pose challenges to unified cyber security governance. International efforts aim to harmonize standards, data protection laws, and privacy norms while respecting national sovereignty and operational differences.

E. Protection of Global Critical Infrastructure: Cyber threats to global supply chains, communications networks, and economic systems prompt multinational efforts to secure transnational infrastructure critical to the functioning of economies and societies worldwide.

XI. CONCLUSION

The cyber security landscape of 2025 is marked by rapidly evolving threats, driven by advances in AI, generative technologies, and expanding attack surfaces from cloud and IOT adoption. Organizations face increasing risks from sophisticated adaptive malware, AI-powered phishing, and deep fake technologies that challenge even the most robust traditional defenses. A significant skills gap, complex regulatory environments, and supply chain vulnerabilities further complicate the fight against cyber threats. To build effective cyber resilience, it is essential for organizations to embrace AI-driven security solutions, foster international collaboration, invest in skill development, and ensure security is embedded by design in all technology initiatives.

RFERENCES

[1] Cyber Security and Applications (Science Direct) | Dr. Rajendra Pamula | Journal Editors | 2025 (in progress) | Vol. 3: Applications, vulnerabilities, mitigation studies | https://www.sciencedirect.com/journal/cyber-security-and-applications/vol/3/suppl/C

[2] Security Week Cyber Insights 2025 | Mike Lennon | Security Week Editorial | Sep 26, 2025 | Cyber security regulation and trends for 2025 | https://www.securityweek.com

[3] 3. SANS Cyber Security Research Papers | Stephen Northcutt | SANS Institute Team | Sep 25, 2025 | Latest research in incident response, threat hunting, and cloud security |https://www.sans.edu/cyber-research/

[4] NIST Cryptographic Module Validation Automation | Dr. Matthew Scholl | NIST Cyber security Division | Sep 25, 2025 | Automation and standards for cryptographic module validation | https://csrc.nist.gov/publications

[5] Journal of Cyber Security (Tech Science Press) | Dr. Mohammed Anbar | Editorial Board | Sep 24, 2025 | Open access, technical/application security research | https://www.techscience.com/journal/JCS

[6] Unit 42 Global Incident Response Report | Philippa Cogswell |Palo Alto Networks | Sep 16, 2025 | Fast evolving multi-vector cyber-attacks and Gen AI phishing | https://unit42.paloaltonetworks.com

[7] Hornet Security Monthly Threat Report |Daniel Hofmann | Hornet Security Analysts | Sep 8, 2025 | AI privacy, SaaS threats, vulnerability and connector exploits | https://www.hornetsecurity.com/en/blog/monthly-threat-report/

[8] Global Data Breaches August 2025 (IT Governance) |Luke Irwin| IT Governance Analysts | Sep 7, 2025 | Recent breaches, exposed records, attack vectors| https://www.itgovernance.co.uk/blog/global-data breaches and-cyber-attacks-in-august-2025-over-17-3-million-records-exposed

[9] The Hacker News Threats Day Bulletin |Mohit Kumar| The Hacker News Staff | Aug 29, 2025 | Weekly cyber news and threat intelligence | https://thehackernews.com

[10] Top Cyber security Threats in 2025 (USD) | Dr. Michelle Moore | USD Cyber security Faculty | Aug 7, 2025 | AI-powered risks, deep fake, evolving malware | https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[11] ENISA Threat Intelligence Publications |Juhan Lepassaar| ENISA Experts | Jun 24, 2025 | EU threat intelligence, cyber regulation, resilience | https://www.enisa.europa.eu/publications

[12] Wipro State of Cyber security Report 2025 |Rohit Adlakha| Wipro Cyber security Team | May 27, 2025 | AI for threat detection, cost optimization, CISO priorities| https://www.wipro.com/newsroom/press-releases/2025/cisos-increasingly-rely-on-ai-to-navigate-cost-pressures-and-enhance-resilience-wipro-report/

[13] Cyber security Case Studies 2025 (EIMT) | Prof. Daniel Gomes | EIMT Research Team | May 22, 2025 | Major global case studies and breach learnings | https://www.eimt.edu.eu/top-best-known-cybersecurity-case-studies

[14] Crowd Strike 2025 Global Threat Report |Adam Meyers| Crowd Strike Intelligence | Feb 26, 2025 | Global threat analysis, incident statistics | https://www.crowdstrike.com/en-us/global-threat-report/

[15] Global Cyber security Outlook 2025 (WEF) | Prof. Dr. Alina Matyukhina | WEF Panel | Jan 26, 2025 | International cooperation, trends, supply chain challenges | https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[16] Checkpoint Cyber Security Report 2025 |Maya Horowitz| Checkpoint Research Labs | Jan 13, 2025 | Attack trends, threat types, mitigation focus | https://www.checkpoint.com/security-report/

[17] Cyber Defense Magazine |Gary S. Miliefsky | Editorial Team | Jan 1, 2025 | Daily cyber defense news and analysis | https://www.cyberdefensemagazine.com

[18] Oxford Academic Journal of Cyber security | Tyler Moore, David Pym |Oxford Cyber security Journal| Dec 31, 2024 | Peer-reviewed interdisciplinary cyber security research | https://academic.oup.com/cybersecurity

[19] Journal of Cyber Security Technology (Taylor & Francis) |Dr. Hani Muheidat| Editorial Board | Sep 30, 2023 | New technologies, defense and application security | https://www.tandfonline.com/journals/tsec20

[20] Slogix Journals of Cyber security |Dr. S. Smys| Slogix Editorial Team | Dec 31, 2023 | Indexed journals, open cyber research listing | https://slogix.in/cybersecurity/leading-journals/