CYBERCRIME TRENDS AND CYBERSECURITY THREATS: EVIDENCE-BASED INSIGHTS FOR LAW ENFORCEMENT AND DIGITAL GOVERNANCE.

Dr. SK Bose

[1*]*Professor School of Law, Manav Rachna University, skbose@mru.edu.in*

Abstract

Cybercrime has emerged as a major challenge to digital security, affecting governments, businesses, and critical infrastructure worldwide. This study examined global cybercrime trends and cybersecurity threats using a quantitative analysis of a publicly available dataset containing 3,000 cybersecurity incidents reported between 2015 and 2024. The research aimed to identify dominant attack patterns, evaluate their financial and operational impacts, and provide evidence-based insights for law enforcement and digital governance. A cross-sectional research design was adopted, and data were analyzed using Python through descriptive and inferential statistical techniques. The analysis focused on attack types, target industries, financial losses, defence mechanisms, affected users, and incident resolution times. The findings revealed that Distributed Denial-of-Service (DDoS) and phishing attacks were the most frequently reported cybersecurity incidents, while information technology and banking sectors experienced the highest attack frequencies. Government organizations incurred the greatest average financial losses, highlighting the vulnerability of critical infrastructure. Differences in incident resolution times across defence mechanisms were relatively small, indicating that effective cybersecurity requires not only technological solutions but also organizational preparedness and coordinated response strategies. The study demonstrates the value of quantitative cybersecurity analytics in supporting evidence-based policymaking, strengthening law enforcement capabilities, and improving digital governance. These findings provide practical guidance for developing proactive cybersecurity strategies to mitigate emerging cyber threats and enhance resilience in an increasingly interconnected digital environment.

Keywords: *cybercrime, cybersecurity threats, law enforcement, digital governance, cybersecurity analytics*

1. INTRODUCTION

The growing adoption of digital technologies, cloud computing, artificial intelligence, connected information systems, and various other technologies has changed modern societies while fostering greater vulnerabilities against cybercrime and cybersecurity threats. Cyber attacks have become a “disciplined” and “organized” activity to government, financial, healthcare, education, and critical infrastructure. Often, these attacks take advantage of technological weaknesses in these systems to disrupt critical services, expose sensitive data and result in significant financial losses. Therefore, cybersecurity has emerged as a key concern for the government, private sector, and international agencies looking to enhance digital resilience and guard against threats to national security (Kuzior et al., 2024; Abdullah et al., 2025).

Recent research shows that the threat landscape is still evolving with increasingly large and sophisticated cyber attacks. Ransomware, phishing, distributed denial-of-service (DDoS), malware and advanced persistent threats have become more prevalent, and they generally cross national boundaries and are outside the scope of the regular law enforcement. However, the international character of cybercrime and the varying capacities of different states to combat cybercrime and their differing legal approaches have made investigation and prosecution more challenging (Chen et al., 2023; Tovkun et al., 2026). With the fast-paced digital transformation in sectors like government and industry, organizations are facing a growing risk of financial damage, disruption, and reputational harm from cybersecurity breaches (George et al., 2024).

Other than purely technical aspects of the problem, cybersecurity remains a relevant question in terms of governance and lawmaking as well. Fast international exchange of data and digitalization of business and service processes have provoked discussions related to issues of privacy, digital sovereignty, and compliance. Legislation that would provide the right balance between cybersecurity and individuals’ rights, international cooperation, and digital governance in general is currently being developed by policymakers (Shi 2025, Laidlaw 2021). At the same time, it becomes increasingly difficult for law enforcement to gather digital evidence, conduct investigations based on it and prosecute cybercrime offenders, especially when they operate across different jurisdictions (Horan & Saiedian, 2021; Grochmal, 2025). This makes it clear that empirical evidence is necessary to make informed decisions in relation to cybersecurity issues.

The changes in the nature of the cybercrime and cybersecurity threats have been extensively examined. With increasingly complex cyberattacks, there is a need for a combined approach that takes into account innovations, policies, and global cooperation (Kuzior et al., 2024). Similarly, Abdullah et al. (2025) were able to illustrate the ways in which historical data of cybercrime could help understand the process of cybercrimes' development and find an adequate solution to cybersecurity problems, underlining the importance of data-based cybersecurity management. Geographical research proved that the distribution of cybercrime was very uneven across countries and regions depending on various factors such as economic development and digital infrastructures (Chen et al., 2023). The research specific to sectors indicates that vital infrastructure such as health care, finance, government, and industry is still very vulnerable to cyber threats because of its critical role and technology connectivity (George et al., 2024; Tovkun et al., 2026).

In the legal aspect, scholars have noted that cyber security governance goes beyond the technical aspects to encompass regulatory compliance and digital privacy, as well as international legal collaboration. Shi (2025) talked about the legal issues regarding cross-border data governance, while Laidlaw (2021) explained the difficulties of harmonizing cybersecurity and privacy in the digital trade landscape. Research on cybercrime investigations has also revealed that there are numerous challenges in collecting digital evidence, conducting digital forensics, and pursuing justice in cross-jurisdictional cases, making it difficult to effectively prosecute cybercriminals (Horan & Saiedian, 2021; Grochmal, 2025). Moreover, recent studies highlighted the need to enhance cybersecurity governance by implementing robust cybersecurity policies and regulations that are harmonized with the law and can effectively address emerging cyber threats (Kausche & Weiss, 2025; Qudus, 2025; Amoo et al., 2024; Santos, 2026).

Although these are also significant, current studies have tended to either concentrate on the technical aspects of cybersecurity events or on discussing legal and governance frameworks conceptually. There are relatively limited empirical studies that combine large-scale, cybersecurity incident data with quantitative analysis that can consider attack trends, economic impacts, victim sectors, security issues, and response strategies and draw conclusions about the implications for law enforcement and digital governance. The lack of such evidence-based knowledge represents an obstacle in the development of strategies that could be used in the prevention of cyber crime and regulation of policy making. In order to address this problem, the current research seeks to quantify the international evidence-based global threat of cyber security on the basis of public international database. Objectives of the current study are as follows:

1. To examine global trends and patterns of cybercrime and cybersecurity threats across countries, industries, and attack categories using quantitative analysis.
2. To evaluate the financial impact, vulnerability characteristics, and incident response mechanisms associated with major cybersecurity incidents.
3. To provide evidence-based insights that support law enforcement strategies and strengthen digital governance for mitigating emerging cyber threats.

2. MATERIALS AND METHODS

2.1 Research Design

Regarding the research methodology used in the study, a quantitative approach has been utilized. In particular, the application of cross-sectional research has been employed for analyzing the trend of cyber attacks and cybersecurity threats on a global scale. This analysis framework was chosen because it allowed uncovering trends of cyber attacks, analyzing their effects, and providing recommendations for law enforcement and digital governance. It is important to note that the quantitative approach has been justified because it allows measuring cybersecurity cases objectively,

comparing different variables statistically, and being replicable.

2.2 Data Source

The dataset was obtained from the Global Cybersecurity Threats (2015-2024) which is publicly available. The data set contains 3000 cybersecurity incidents from 2015 to 2024, providing details on countries, years, type of attacks, industry attacked, monetary loss, number of users affected, attack source, security vulnerability type, defense mechanisms used and time taken to resolve the incident (Soundankar, 2025). The data do not contain any identifiable information, and they were gathered for research and analysis study, which is suitable for secondary quantitative analysis.

2.3 Data Preparation

The data set was explored for completeness and consistency, and for analytical suitability, before the analysis. Duplicate entries, missing data, and inconsistencies in categorical information were detected and screened from the records. The names of the variables were unified, the categorical variables were codified as needed to be used in the computational analysis, and the numerical variables were checked for their data types. All data had none missing and needed little to no modification prior to statistical assessment.

2.4 Statistical Analysis

Data analysis was conducted using Python (Version 3.12), inferential and descriptive. Data manipulation and data preprocessing were carried out using Pandas Library, whereas the calculations were carried out using NumPy Library. For summarization of the cyber incidents, descriptive statistics, including frequencies, percentages, means, and standard deviation, were calculated. Correlation analysis was carried out to find out the relationship between the study variables, and comparative analysis was conducted for studying the differences between attack types, industries, and defensive measures. For the purposes of visualization of the cybersecurity incidents, graphs were developed using Matplotlib and Seaborn. When statistical analysis was applied, the significance level was set at 95%.

2.5 Machine Learning Analysis

Machine Learning methods were used in order to analyze the relationship that exists between the different variables in the cybersecurity data. The languages that were used in developing these models were Python and the Scikit-learn library. Three different models were constructed namely Decision tree, Random Forest and Extreme Gradient Boosting (XGBoost). These models were constructed for the purpose of relating the cybersecurity results with the attack characteristics, vulnerability types, industry sectors and defensive measures. The performance of these models was assessed using the five commonly known evaluation parameters; accuracy, precision, recall, F1-Score and ROC-AUC.

3. RESULTS

3.1 Global Distribution of Cybercrime Trends and Cybersecurity Threats

In order to conduct an analysis of the global trend in cyber crime incidences, 3,000 cybersecurity cases were analyzed which took place from 2015 to 2024. The information for the research was gathered from different countries and various industries and it included all sorts of cyber crimes. There are basically five types of attacks identified; Distributed Denial of Service (DDoS) attack, Phishing attack, Ransomware attack, Malware attack and Man in the Middle attacks. DDoS and Phishing attacks are the most common of all (refer to Figure 1). Likewise, the results from Table 1 indicate that DDoS (n = 531) and Phishing (n = 529) attacks had the highest and the second highest frequencies, respectively, while Man-in-the-middle attacks had the lowest frequency (n = 459). The average number of financial losses reached USD 49 million in all attack categories, illustrating the significant economic impact of today's cybercrime. The relative frequency of the categories of major cyber attacks is shown in figure 1, where it is evident that the majority of major attacks during the study period were comprised of DDoS and phishing attacks.

Table 1. Distribution of Cybersecurity Incidents by Attack Type

Attack Type	Number of Incidents	Mean Financial Loss (Million USD)	Mean Affected Users
DDoS	531	52.04	499,437
Phishing	529	50.46	487,180
Ransomware	493	49.65	502,825
Malware	485	49.42	508,780
Man-in-the-Middle	459	51.31	520,064

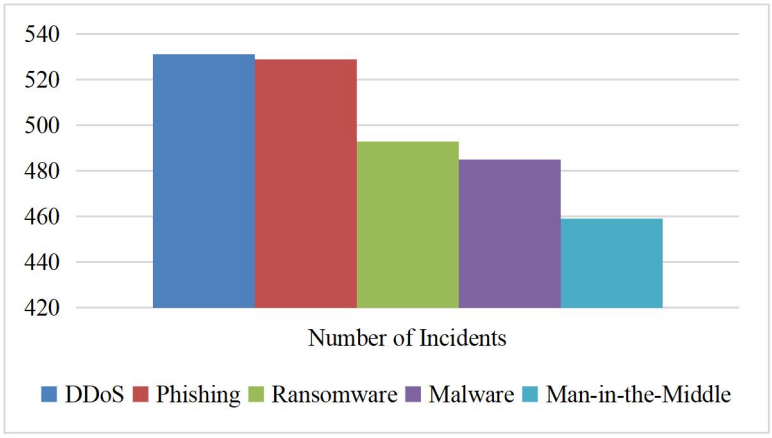

Figure 1. Global Distribution of Cybersecurity Incidents by Attack Type

3.2 Sectoral Impact of Cybersecurity Threats

A variety of critical industries were involved in the cybersecurity incidents, such as banking, healthcare, information technology, retail, education and government services. As shown in Table 2, the information technology was the industry with the highest reported incidents (n = 478) and the government was the industry with the highest average financial loss (USD 52.62 million). Incident resolution times were, on average, between about 35 and 38 hours, across sectors, suggesting that, despite varying attack frequencies and economic impacts, the response time was comparable. Government, IT and banking industries were always observed to have higher financial losses than other sectors, which represent the attractiveness of these sectors to the cybercriminals and their strategic importance.

Table 2. Sector-wise Distribution of Cybersecurity Incidents and Financial Impact

Target Industry	Number of Incidents	Mean Financial Loss (Million USD)	Mean Resolution Time (Hours)
IT	478	51.90	36.17
Banking	445	51.17	35.74
Healthcare	429	49.05	35.81
Education	419	47.90	35.91
Government	403	52.62	37.59

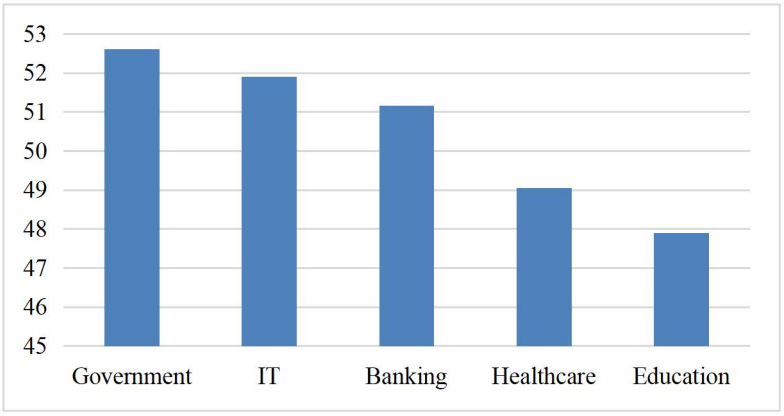

Figure 2. Mean Financial Loss Across Target Industries

3.3 Defensive Mechanisms and Incident Response Performance

The frequency of use of defensive mechanisms and their corresponding incident resolution times were used to evaluate the effectiveness of defensive mechanisms. There are five key defence mechanisms: antivirus software, virtual private networks (VPNs), firewalls, encryption technologies, and artificial intelligence (AI) based detection. According to Table 3, the most common defence mechanism used is a VPN (n = 612), while AI based detection systems were used in 583 incidents. The average incident resolution time was fairly similar (35.71 to 36.86 hours) for the various defence mechanisms. The average incident resolution time of various cybersecurity defence mechanisms is shown in Figure 3, where the operational performance does not vary significantly, and the time to resolve incidents after deployment of the firewall is slightly lower.

Table 3. Distribution of Defence Mechanisms and Incident Resolution Time

Defence Mechanism	Number of Incidents	Mean Resolution Time (Hours)
VPN	612	36.86
Antivirus	628	36.57
Encryption	592	36.59
Firewall	585	35.71
AI-based Detection	583	36.61

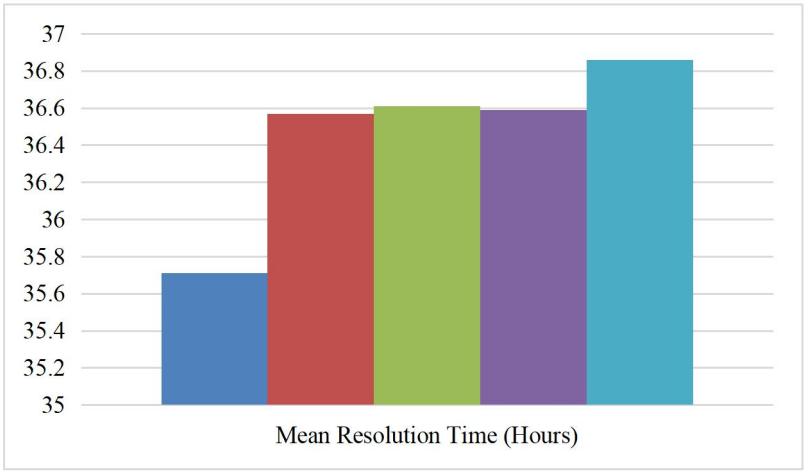

Figure 3. Comparison of Average Incident Resolution Time Across Defence Mechanisms

4. DISCUSSION

Cybersecurity incident reports between the years 2015 and 2024 are compiled in this study and examined to determine the trends and cybersecurity threats facing the world. It is found that Distributed Denial of Service (DDoS) and Phishing attacks were the two most prevalent forms of attacks recorded, showing how relevant they have been to the cyber world up till now. This finding agrees with the study conducted by Kuzior et al. (2024), where it was found that cyber criminals were focusing on exploiting vulnerabilities in the networks and using social engineering methods due to their effectiveness in disrupting the functioning of any company. In a similar study, it was found by Abdullah et al. (2025) that phishing and DDoS attacks are one of the most persistent cybercrimes despite the advances in cybersecurity tools and techniques.

The results from the sectoral analysis showed that different organizations such as information technology, banking had the most frequent cyber security incidents while governmental organizations had the highest average financial losses. This aligns with earlier studies that have shown that critical infrastructure industries continue to be lucrative targets due to the significant and valuable digital assets, and the critical public services they manage (George et al., 2024; Adisa, 2023). The economic impact illustrated in the current study also highlights that cybercrime is not just a matter of technical disruption, but is a key economic and national security challenge as well. Improving preparedness and risk management measures for cybersecurity at a sectoral level is therefore key to minimising the vulnerability of organisations and maintaining continuity of critical services.

Another significant discovery is the relatively small differences between the incident resolution times of different defence mechanisms. The protection via a firewall showed slightly lower response times compared to the other means of protection, but the difference was not significant. This indicates that the success of cybersecurity responses is not as much based on individual technological controls but on organizational preparedness, coordination of the incident response efforts and cyber security awareness. De Kimpe et al. (2022) pointed out the strong link between the effectiveness of cybersecurity and users' knowledge, their trust in the system, and their protective action, and Althibyani and Al-Zahrani (2023) showed that digital citizenship and cybersecurity awareness play a significant role in preventing cybercrime. Therefore, investment in cybersecurity education and competency of the workforce should be part of technological security solutions.

The results have significant implications for law enforcement and digital government. Cyberattacks happen at both national and international level and in various sectors, which highlights the transnational character of cybercrime and poses significant problems in the investigation of cybercrime, the collection of digital evidence and cross-border legal cooperation. It has been noted by Afzal (2024) that the problem of complexity of digital law enforcement in the modern technological environment exists as well. Gaskell (2024) further suggested that due to the development of new digital technologies, including artificial intelligence, there appear new ethical and operational problems that should be updated all the time. In a similar way, Alhajeri (2022) argued that improving the digital skills of the law enforcement officers is crucial for the protection of critical infrastructures from emerging cyber threats. Thus, the importance of continuous learning and international cooperation in the field can be seen.

In terms of governance, it illustrates that quantitative cybersecurity evidence can be used to inform policy making, by highlighting which industries are most at risk, the most popular attack vectors and which areas are vulnerable. Strong network security governance should be facilitated by aligned legislation, inter-agency cooperation, and evidence-informed policy making that can meet the ever-changing nature of cyber threats. Mushtaq and Shah (2024) highlighted that a holistic approach to cybersecurity governance can be a great asset in strengthening the resilience of public services, especially in digital government. Likewise, Al-Husaini (2024) emphasized the need for enhanced collaboration between law enforcement agencies and cloud service providers to enhance digital forensic investigations and incident response. Such views are in line with our present results, which indicate that cybersecurity policies should be based on technological protection as well as legal, organizational and institutional protection in order to increase cyber resilience.

The overall conclusion of this study is that it can add empirical evidence to link the characteristics of cybersecurity incidents to issues of cybercrime prevention, law enforcement and digital governance. The worldwide analysis of cybersecurity incidents provides insights into some of the most common and devastating cybersecurity incidents in different industrial domains and different types of attacks, which might be useful for policymakers, cyber security experts,

and even law enforcement agencies to make decisions about prioritization of cyber security measures and creation of evidence-based cyber security laws. Further research can be conducted based on this study through the use of longitudinal data and threat intelligence/ legal enforcement indicators.

5. CONCLUSION

In this research paper, an attempt is made to carry out a data based assessment of dynamics and risks of cyber crime by doing an empirical analysis of cyber security incidents reported during the period between 2015 and 2024. The research has been found to show that DDoS attacks and phishing attacks remain the most prevalent cyber threats and the important sectors such as information technology, banking and government suffer greatly in terms of their operations and finances. While several different defense mechanisms have been employed, there were little differences in the duration of resolution of incidents and this indicates the requirement of good cybersecurity which is possible only when there is a right mixture of technological tools, preparedness of organizations and incident response skills. In addition, it is imperative to use empirical research on cybersecurity for law enforcement and digital governance for enhancing cyber resilience and effective policy making. The findings of this research can be used by policymakers, cyber security experts and regulatory authorities in prioritizing preventive efforts and resource allocation by identifying important attack patterns, vulnerable segments and incident response characteristics

Reference

1. Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. Analytics, 4(3), 25.
2. Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.
3. Afzal, J. (2024). Digital law enforcement challenges and improvement. In Implementation of digital law as a legal tool in the current digital era (pp. 47-78). Singapore: Springer Nature Singapore.
4. Alhajeri, M. (2022). Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI). University of Salford (United Kingdom).
5. Al-Husaini, Y. (2024). Enhancing cloud forensic investigation relationships between law enforcement and local cloud service providers: Oman as a case study (Doctoral dissertation, RMIT University).
6. Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. Sustainability, 15(15), 11512.
7. Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205-217.
8. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10(1), 71.
9. De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808.
10. Gaskell, A. R. (2024). Towards Understanding the Ethical and Operational Implications of Large Language Models in a Law Enforcement Environment (Doctoral dissertation, Macquarie University).
11. George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51-75.
12. Grochmal, A. B. (2025). Challenges Faced by Law Enforcement Collecting and Using Digital Evidence in Cybercrime Investigations (Doctoral dissertation, Marymount University).
13. Horan, C., & Saiedian, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. Journal of Cybersecurity and Privacy, 1(4), 580-596.
14. Kausche, K., & Weiss, M. (2025). Platform power and regulatory capture in digital governance. Business and Politics, 27(2), 284-308.
15. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies (2071-8330), 17(2).
16. Laidlaw, E. (2021). Privacy and cybersecurity in digital trade: The challenge of cross border data flows. Available at SSRN 3790936.
17. Mushtaq, S., & Shah, M. (2024). Critical factors and practices in mitigating cybercrimes within e-government services: A rapid review on optimising public service management. Information, 15(10), 619.
18. Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. International Journal of Science and Research Archive, 14(1), 1146-1163.
19. Santos, C. P. (2026). Global Cybersecurity Governance: Challenges in Harmonizing International Cyber Laws. Journal of Intelligent Decision Making and Information Science, 3(3s), 1874-1893.
20. Shi, Y. (2025). Risk Prevention in Global Cross-Border Data Flows: Challenges and China's Strategic Responses. International Journal of Digital Law and Governance, 2(2), 373-399.
21. Soundankar, A. (2025). Global cybersecurity threats (2015–2024) [Data set]. Kaggle. https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024
22. Tovkun, Y., Semerenska, V., & Adamov, A. (2026). An overview of cyber attacks on critical cyber-physical systems and government infrastructures. Security and Safety, 5, 2026002.