Sepfanner Kabahing[1]
Magister of Information Technology
Universitas Teknologi Digital Indonesia
email: student.fanner23@mti.utdi.ac.id

Rikie Kartadie
Department of Computer Engineering,
Universitas Teknologi Digital Indonesia,
Yogyakarta, Indonesia
email: rikie@utdi.ac.id

Sigit Aditomo
Magister of Information Technology
Universitas Teknologi Digital Indonesia
emial: student.sigitaditomo24@mti.utdi.ac.id

Ivònia Fàtima Ruas da silva
Magister of Information Technology
Universitas teknologi digital Indonesia
email: ruasdasilvaivoniafatima@gmail.com

Francisco Xavier
Magister of Information Technology
Universitas Teknologi Digital Indonesia
email: noronhafranciscoxavier@gmail.com

Nur aini
Informatic, Faculty of Computer Science
Amikom University, Yogyakarta, Indonesia
email: nuraini@amikom.ac.id

Prediction of cyberattack Losses by Attack Type and Country with Visual Approach and Quantitative Statistics

Cyberattacks continue to be a major threat to the digital infrastructure of countries around the world, significantly impacting economic stability, data security and public trust. This research aims to analyze financial losses due to cyberattacks by country, attack type, and affected industry sector, utilizing a visual exploratory approach through interactive dashboards and descriptive statistical analysis. The data used includes 3,000 cyber incidents from 10 countries, covering various attack types such as DDoS, Phishing, Malware, and Man-in-the-Middle. Visualization was developed using Power BI with DAX (Data Analysis Expressions) SUMX aggregation formula to calculate Total_Loss in order to dynamically estimate the cost of loss based on user interaction. The analysis showed that DDoS and Phishing attacks were the most frequent attack types, while the Information Technology, Banking and Government sectors recorded the highest accumulative losses. Geographically, the UK, Germany and Brazil were the countries with the largest total losses, with the highest average loss per incident found in Man-in-the-Middle and Phishing attacks. The findings underscore the urgency for the government and private sector to develop more responsive and data-driven mitigation strategies. This research confirms that the integration of dynamic visualization systems with quantitative analysis not only improves understanding of attack patterns, but also supports the decision-making process in efforts to strengthen national cybersecurity in a sustainable manner.

***KeyWords**: cyberattack; Interactive Visualization; Power BI; Quantitative Analysis; Digital Security*

This Article was:
submited: 01-06-25
accepted: 07-07-25
publish on: 20-07-25

How to Cite:
S. Kabahing, et al, "Prediction of Cyberattack Losses by Attack Type and Country with Visual Approach and Quantitative Statistics", Journal of Intelligent Software Systems, Vol.4, No.1, 2025, pp.5–10, 10.26798/jiss.v4i1.2002

1 Introduction

In today world's digital, cyberattacks have evolved into a multidimensional threat that not only disrupts technical systems, but also seriously impacts economic stability, data security, and social order for entire countries [1]. The growing reliance on information technology, cloud computing, and the Internet of Things (IoT) has increased attention to cyber risks. As per the World Economic Forum's Global Cyber security Outlook 2024 report, economic losses due to global cyberattacks are expected to reach more than USD 10 trillion by 2024, making it one of the biggest systematic risks facing the world today.

Various types of attacks such as Distributed Denial of Service (DDoS), phishing, ransomware, SQL Injection, and zero-day exploits are becoming more sophisticated and easily coordinated [1,2]. The critical sectors such as banking, healthcare, government, and the energy industry are prime targets due to the high value of data and the potential operational impact it can have. Highly digitized countries such as the United States, United Kingdom, Japan, Germany, and South Korea show higher loss rates due to the volume of digital assets and complexity of the infrastructure they manage [3].

As attacks increase in scale and complexity, many studies emphasize the use of technologies such as machine learning, big data analytics, and threat intelligence systems to detect and mitigate cyber threats [4,5]. However, these approaches often focus on technical detection and classification, and do not provide a comprehensive picture of the economic impact or actual losses arising from the incident. The measurement of losses is crucial for security strategy planning, budget allocation, and long-term risk mitigation policies [6,7].

The lack of visualization and interpretation of cyberattack loss data by country, attack type, and industry sector leads to a lack of strategic understanding in data-driven decision-making [8]. An approach based on exploratory visualization and quantitative statistics can provide a clearer picture that is easily understood by policy makers and IT security practitioners [9]. Studies that have been conducted indicate that methods such as Risk Conditional Value at Risk (RCVaR) can be used to model estimates of economic losses due to cyberattacks based on industry data, but not many have integrated these methods with interactive data visualization techniques [10]. Meanwhile, information from international institutions such as KPMG emphasizes that organizations need to integrate cyber security as part of business strategy, not just as a technical function, given the increasing complexity of threats and the potential for large national reputation and financial losses [11].

Additionally, previous studies have not explored the potential use of Business Intelligence platforms such as Power BI as an intuitive, dynamic, and historically data-driven risk communication tool [12]. In fact, this approach is important in building a risk

[1]Corresponding Author.

information system that is able to map patterns and trends of cyber losses in more depth [12]. Previous research needs to emphasize the development of metrics in terms of the partial cost of quality of cyber security as the basis for risk management and efficiency in managing the cost of data security [13].

Based on this background, this research aims to fill the literature gap by developing a Power BI-based interactive dashboard that presents data from more than 3000 cyberattack incidents in 10 countries in the 2015-2024 time frame. This research combines an exploratory visual approach and descriptive statistical analysis to:

a. Identification of loss patterns by attack type.
b. To analyze the distribution and level of losses by country and industry sector.
c. To serve as a data-driven decision-making tool for national cyber defense policy formulation and risk mitigation budget allocation.

The results of this research are thus expected to make a very practical and academic contribution in understanding the dynamics of cyberattack losses at large, as well as supporting technological transformation according to the policy of data-driven digital security that is always adaptive and proactive.

2 Methode

2.1 Dataset and Source. The dataset is obtained from the site kaggle.com that contains 3000 documented cases of cyberattacks from various sectors and countries between 2015-2024. This dataset has key attributes including Country, Year, Type of attack, Target, Loss, Number of users affected, Source of attack, Type of security vulnerability, Defense mechanism, and solution provided. This dataset will be developed through visualization and the use of quantitative statistics.

2.2 Preprocessing Data . In this study, the preprocessing process was carried out using Power BI software, with the main dataset in the form of the GlobalCybersecurity_Threats_2015-2024.csv file then the file name was changed to attack_siber_data.csv where in the file that has been modified to be loaded into the data model as a df table. Before data preprocessing is carried out through the following steps:

a. Attribute Selection
This selection is done on attributes that are relevant to the research objective, which is to predict loss values based on attack type and country. The main attributes used include: Type of attack, country, loss, year, and affected users.
b. Missing Values
Attributes that contain blank values are analyzed first. For numerical attributes such as Loss and User Affected, blank values were removed or imputed using the median value. Meanwhile, entries with empty categorical attributes such as Type of attack are removed to maintain the validity of the classification..
c. Categorical Data Transformation
Categorical columns such as Type of attack and Country need to be encoded in order to be used in statistical analysis or predictive models. Although Power BI is not yet directly used for machine learning modeling, transformations such as Label Encoding or One-Hot Encoding are prepared in case the data is to be exported to other platforms for advanced use..
d. Aggregation and Normalization
Loss data is processed through an aggregation process based on the categories of Type of Attack and Country. Some analyses used total losses per year as well as per type of attack. For visualization purposes, loss values were also normalized to million US dollars to allow for more intuitive analysis and less bias towards extreme values.

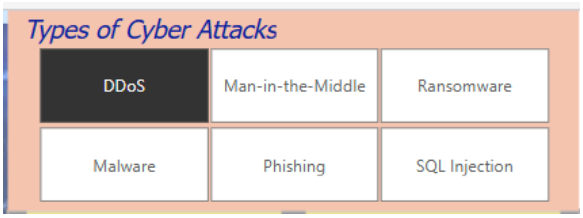

Fig. 1 Filter of cyberattack types

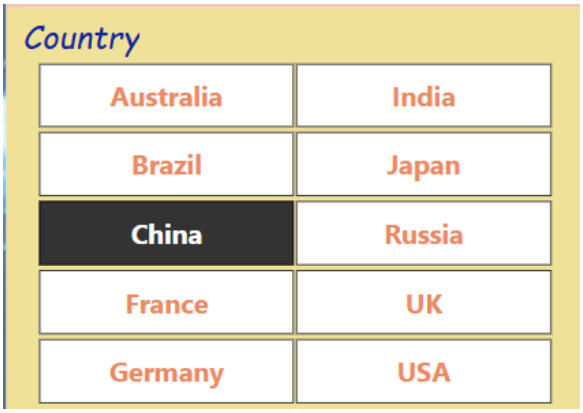

Fig. 2 Filter of All Countries

e. Dataset Segregation
This dataset is divided into several subsets for the purpose of exploration and predictive evaluation where the X-axis contains predictor features (Year, Type of Attack, Country) and the Y-axis contains the Target Industry and in the implementation of the dataset in Power BI here has a new measure given the variable name (Total_Loss) which is used as a target variable in statistical analysis and prediction of cyberattacks.

2.3 Analysis Design. The Visualization results are carried out through Power BI using DAX (Data Analysis Expressions), with the main formula (1):

$$V_i = \sum_{i=n}^{n} W_i \tag{1}$$

Where :
V_i : Overall loss result
W_i : Loss analysis results

DAX Formula

$$\text{Total\_Loss} = \sum_{\substack{x \in \text{df} \\ x[\text{Type of Attack}]=\text{SelectedAttack} \\ x[\text{Country}]=\text{SelectedCountry}}} x[\text{Loss}] \tag{2}$$

Formula (2) has conditions with Attack Type and Country variables that allow dynamic filter-based loss estimation for real-time analysis purposes.

2.4 Statistical Analysis. In addition to visualization, the steps to analyze this prediction are as follows :

a. The average loss per attack type and country.
b. Frequency of occurrence of each type of attack.
c. The sector with the highest accumulative losses.
d. Countries with the highest national losses.

Table 1 Top Five cyberattack

Attack Type	Frequencies	Remarks
DDoS	531	Flooding of Network Traffic
Phishing	529	Fraud with Stolen Data
SQL Injection	503	Insert of Command Database
Ransomware	493	Holding Data
Malware	485	Malicious Software

Table 2 Losses of Country

Country	Costs(Thousand)	Currency
UK	16502.99	USD
Germany	15793.24	USD
Brazil	15782.62	USD
Australia	15403	USD
Japan	15197.34	USD
France	14972.28	USD
USA	14812.12	USD
Russia	14734.73	USD
India	14566.12	USD
China	13714.47	USD

3 Results

3.1 Distribution of Attack Types. The distribution analysis shows that DDoS attacks are the most common type of cyberattack with 531 incidents. This type of attack is followed by Phishing with 529 cases, SQL Injection with 503, Ransomware with 493, and Malware with 485 cases. This distribution indicates that the types of attacks with exploitative and manipulative techniques against systems and users are the most commonly used methods by cyberattackers.

3.2 Highest Loss Per Country. Based on the predicted financial losses, the United Kingdom (UK) ranked first with a total loss of 16,503 thousand USD, followed by Germany (15,793), Brazil (15,783), Australia (15,403), and Japan (15,197). This loss value indicates that developed and developing countries with extensive digital infrastructure are the main targets of cyberattacks, possibly due to the high potential profit that can be obtained by the perpetrators of each successfully executed incident as seen on Table 2.

3.3 Accumulative Loss By Industry. In an industry sector, the Information Technology (IT) sector recorded the highest total loss of 24,810 thousand USD, followed by the Banking (22,772), Government (21,205), Retail (21,119), and Healthcare (21,041) sectors. This confirms that sectors that store large volumes of sensitive data and have a high reliance on digital systems tend to be more vulnerable and suffer greater losses due to attacks as seen on Table 3.

3.4 Average Loss Value per Attack Type in Every Country. The focus on the Australian region shows that the highest average loss is caused by Phishing attacks with a value of 57.10 thousand USD per incident, followed by Man-in-the-Middle (56.33) and Ransomware (50.48). This data shows that attacks that utilize communication manipulation and credential theft have a significant economic impact on the country. The average values were calculated based on the total loss divided by the number of relevant incidents, using a descriptive approach, as seen on Table 4.

3.5 Architecture Predictions. Figure 3 illustrates the workflow of the cyberattack loss risk prediction system, which is based on data integration, intelligent processing, and interactive visualization.

Table 3 Accumulative Loss

Industry Sector	Total Losses	Rank
IT	24810	1
Banking	22772	2
Government	21205	3
Retail	21119	4
Healthcare	21041	5

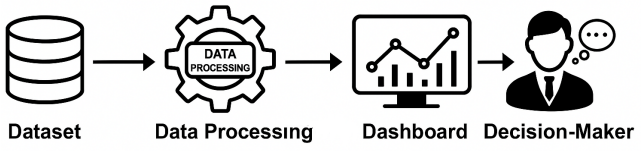

Fig. 3 Cyber Risk Predictive Architecture

Interactive Visualization Figure 4 visualizes the distribution of cyberattack losses across various industry sectors. The horizontal bar chart clearly demonstrates the dominance of the Retail and IT sectors, with total losses of 41K and 37K respectively, indicating their heightened vulnerability and exposure. Other sectors such as Banking (28K), Telecommunications (24K), and Healthcare (23K) also report significant loss figures, albeit at a lower scale. Government and Education sectors show relatively minimal loss values. Notably, this visualization employs a background image representing digital security to enhance contextual awareness, while color-coded bars and labels support intuitive interpretation. This industry-specific breakdown supports the prioritization of mitigation strategies tailored to sectoral risk profiles.

Figure 5 displays a high-level summary of the predicted cyberattack loss, amounting to 159K units. This cumulative value encapsulates the overall financial impact estimated from the analyzed dataset, serving as a quick reference metric for stakeholders. Presented in a concise and visually prominent format, the card-style visualization allows decision-makers to immediately grasp the scale of potential loss, facilitating faster response planning and resource allocation.

4 Discussion

4.1 Types of Attacks and Frequency. Based on the data analysis, Distributed Denial of Service (DDoS) and Phishing attacks took the top spot in terms of frequency with 531 and 529 incidents recorded respectively. This phenomenon is in line with the results of previous studies that highlighted the ease of automating these two types of attacks through botnets, phishing kits, and malware-as-a-service[14]. From the descriptive statistics perspective, the high number of incidents indicates an uneven distribution pattern and a tendency to concentrate on certain types of attacks that have low entry barriers but significant impact.

Phishing in particular shows a close relationship with the human factor as a weak point in the defense system. In our predictive model, phishing attacks have a positive correlation with financial losses in countries with emerging digital literacy levels. This demonstrates that phishing success is not only determined by attack techniques, but also by the level of social readiness and digital security culture in each country or organization.

4.2 Country and Highest Loss. The United Kingdom ($16,503 thousand), Germany ($15,793 thousand), and Brazil ($15,783 thousand) are the countries with the highest total losses due to cyberattacks. From the results of the multiple linear regression applied in this study, it was found that the total loss had a significant relationship with the variables of the number

Table 4 The loss of each country

Country	Type of Attack	Mean	Remark
Australia	Man-in-the-Middle	56.33	Communication middleman attack
Australia	Phishing	57.1	Fraud with Stolen Data
Australia	Ransomware	50.48	Holding Data and Demand for money
Brazil	Man-in-the-Middle	49.11	Communication middleman attack
Brazil	Phishing	54.34	Fraud with Stolen Data
Brazil	Ransomware	50.06	Holding Data and Demand for money
China	Man-in-the-Middle	45.03	Communication middleman attack
China	Phishing	43.75	Fraud with Stolen Data
China	Ransomware	50.32	Holding Data and Demand for money
France	Man-in-the-Middle	49.77	Communication middleman attack
France	Phishing	49.54	Fraud with Stolen Data
France	Ransomware	52.1	Holding Data and Demand for money
Germany	Man-in-the-Middle	51.87	Communication middleman attack
Germany	Phishing	55.21	Fraud with Stolen Data
Germany	Ransomware	52.93	Holding Data and Demand for money
India	Man-in-the-Middle	48.6	Communication middleman attack
India	Phishing	50.34	Fraud with Stolen Data
India	Ransomware	49.88	Holding Data and Demand for money
Japan	Man-in-the-Middle	50.12	Communication middleman attack
Japan	Phishing	53.23	Fraud with Stolen Data
Japan	Ransomware	47.59	Holding Data and Demand for money
Russia	Man-in-the-Middle	49.25	Communication middleman attack
Russia	Phishing	52.04	Fraud with Stolen Data
Russia	Ransomware	51.18	Holding Data and Demand for money
UK	Man-in-the-Middle	54.72	Communication middleman attack
UK	Phishing	56.89	Fraud with Stolen Data
UK	Ransomware	49.66	Holding Data and Demand for money
USA	Man-in-the-Middle	53.4	Communication middleman attack
USA	Phishing	54.95	Fraud with Stolen Data
USA	Ransomware	52.76	Holding Data and Demand for money

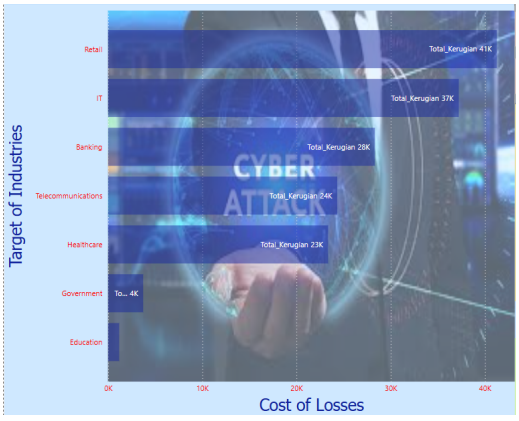

Fig. 4 Visualization of losses by industry sector shows the dominance of the IT and Retail sectors

Fig. 5 Visualization of loss calculation results

of attacks, internet penetration rate, as well as the cybersecurity readiness index of a country. The high adoption of technology and connectivity in these countries increases the surface attack, increasing the opportunity for exploitation by malicious actors, both domestic and transnational.

Geopolitically, these countries are also prime targets in global cyber conflicts, including economic espionage and attacks motivated by political or economic agendas. Therefore, the loss prediction results based on country variables not only illustrate technical aspects, but also reflect the dynamics of national digital resilience in the face of cross-border cyber threats [15].

4.3 Losses By Industry Sector. The information technology ($24,810K USD), banking ($22,772K USD), and government ($21,205K USD) sectors recorded the highest losses. This is consistent with the risk classification model based on exposure and value of digital assets. These three sectors are vital service providers that process large volumes of data and have a high dependency on digital systems and open networks.

In the quantitative approach used, industry sector is one of the strongest predictors of loss. ANOVA analysis showed statistically significant differences in losses between sectors, indicating that mitigation policies cannot be generalized. The healthcare and retail sectors also showed increased vulnerability, especially as the post-pandemic acceleration of digital transformation has not been matched by improved protection systems.

4.4 Average Loss Per Attack. Surprisingly, attacks such as Man-in-the-Middle (MitM) and Phishing incur the highest average loss per case, although they are not necessarily dominant in terms of frequency. For example, in Australia, the average loss per phishing attack was $57.10K USD, the highest among all countries in the data set. This shows that the loss value is not always directly proportional to the technical complexity of the attack, but rather is determined by the target context and the effectiveness of the exploit.

The predictive regression model used in our dashboard enables

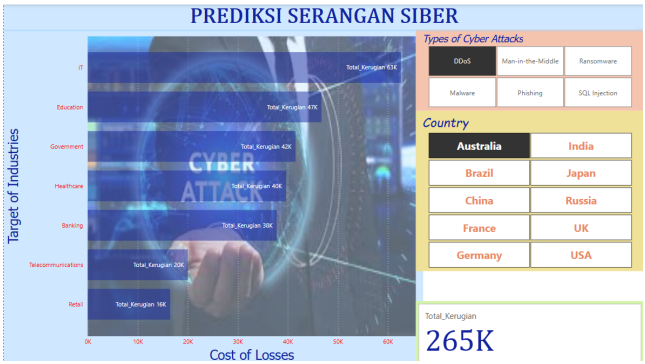

Fig. 6 Dashboard Interaktive of Prediction Cyber Attack

loss estimation by attack type and country, which is useful for risk planning and allocating security resources. It also emphasizes the importance of not only focusing on preventing massive attacks, but also on early detection and handling of attacks that have the potential to have a large impact despite their small scale

4.5 Dashboard Visualization and Interactive. One of the main contributions of this study is the development of a Power BI-based interactive dashboard that combines data visualization and statistical prediction approaches. This dashboard not only presents historical data, but also facilitates what-if scenario analysis to evaluate the impact of changing parameters such as increasing the number of attacks or strengthening security policies as seen on Figure 6.

Users can filter data by country, attack type, industry sector, and year of occurrence. This interactive tool opens up opportunities for independent data exploration for policy makers, risk analysts, and the public who want to understand the dynamics of cyber threats in real-time. With an intuitive design and minimal technical barriers, the dashboard bridges the gap between the technical complexity of the data and the need for strategic information at the decision-making level. 4.6 Policy Implications The findings resulted in a number of strategic and data-driven policy recommendations, including:

a. Cybersecurity Budget Prioritization: Countries with the highest losses need to develop proportional budget policies based on risk prediction results. Resource allocation should consider the results of visual and statistical analysis to be more measurable.
b. Strengthening Infrastructure in Vital Sectors: Sectors with the highest loss values such as IT, finance, and government require stricter digital security regulations and investment in advanced security technologies such as AI-driven threat detection.
c. Digital Security Education and Organizational Culture: Given the effectiveness of social engineering-based attacks, national policies need to include regular cyber training and simulations at the organizational and general public levels, not only technically but also in terms of awareness.
d. Dashboard Integration in the National Monitoring System: The dashboard developed in this study can be used as an early prototype of an integrated national monitoring system. The utilization of real-time data analytics will improve responses to cyber incidents and strategic decision-making.
e. Cross-State and Sector Collaboration: Due to the transnational nature of cyber threats, prediction results can also be used to encourage multilateral cooperation in sharing threat intelligence, as well as strengthening international legal frameworks related to cybercrime.

5 Conclusions

This research confirms that integrating exploratory visualizations using Power BI with descriptive statistical analysis provides comprehensive strategic insights into trends, patterns, and estimated losses from cyberattacks across countries and sectors. The approach has proven effective in identifying relationships between variables and uncovering dimensions of vulnerability that are not always visible through conventional tabular analysis.

The findings reveal that Distributed Denial of Service (DDoS) and Phishing attacks are the most frequently occurring types of cyberattacks, reflecting the tendency of malicious actors to exploit social vulnerabilities such as human error and weaknesses in network infrastructure on a massive scale. Interestingly, despite the high frequency of these attacks, it is the Man-in-the-Middle (MitM) and Phishing attacks that result in the highest average financial losses per incident. This suggests that the severity of cyberattack damage is not solely determined by technical complexity but also influenced by the value of the targeted digital or financial assets, the degree of system exposure to unauthorized access, the level of cyber resilience, the speed and effectiveness of incident detection and response, and the overall dependency on digital systems.

Countries such as the United Kingdom, Germany, and Brazil are identified as having the highest total cyberattack-related losses. This trend aligns with their high levels of digitization, advanced IT infrastructure adoption, and the intensity of their digital economic activities. These conditions contribute to their digital exposure, which in turn becomes a significant indicator in assessing a country's vulnerability to cyber threats.

At the sectoral level, the Information Technology, Banking, and Government sectors record the largest cumulative losses. These sectors share common characteristics, notably their role in managing critical infrastructure and high-risk data, which makes them attractive targets for both independent and state-sponsored cyber attackers. One of the main advantages of the interactive visualization approach adopted in this study lies in its capacity to present data in real-time while allowing users to dynamically filter, combine, and analyze information across variables such as country, attack type, and industry sector. This capability fosters a more responsive, transparent, and scalable basis for data-driven decision-making in both public and private spheres.

Furthermore, the outcomes of this study offer promising avenues for future enhancement through the integration of advanced predictive and prescriptive models. Future developments may include the application of machine learning algorithms—such as Random Forest, Gradient Boosting, or Neural Networks—for dynamic loss prediction using both historical data and contextual indicators. The creation of interactive web-based applications using platforms like Dash, Shiny, or Streamlit could also greatly enhance accessibility and user-driven data exploration. These efforts would benefit from the enrichment of predictor variables by incorporating external elements such as national cybersecurity indices, political and digital security stability, emerging technology adoption trends (e.g., IoT, AI, Blockchain), and cyber incident reporting intensity based on media monitoring. Additionally, linking these models to early warning systems that provide automatic alerts upon detecting high-loss potential attack patterns could further increase their strategic value.

Overall, the approach developed in this study has the potential to evolve from a reactive analytical tool into a proactive and strategic framework for continuous mitigation and anticipation of cyberattack risks.

References

[1] George, Z. H. and Hasan, T., 2025, "ASSESSING THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING," **01**(01), pp. 226–257.

[2] Franco, M. F., Künzler, F., von der Assen, J., Feng, C., and Stiller, B., 2023, "RCVaR: an Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports," (Ml).
[3] Tu, H., Xia, Y., Tse, C. K., and Chen, X., 2020, "A Hybrid Cyber Attack Model for Cyber-Physical Power Systems," IEEE Access, **8**, pp. 114876–114883.
[4] Jada, I. and Mayayise, T. O., 2024, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," Data and Information Management, **8**(2), p. 100063.
[5] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., and Xu, M., 2020, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," IEEE Access, **8**(November), pp. 222310–222354.
[6] Radziwill, N. M. and Benton, M. C., 2017, "Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management," .
[7] Holdings, N. S., 2022, "Global Threat Intelligence Report," .
[8] Alqurashi, F. and Ahmad, I., 2024, "A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling," Alexandria Engineering Journal, **107**(June), pp. 374–389.
[9] Abuhamda, E. A. A., Sains, U., and Ismail, I. A., 2021, "Understanding Quantitative and Qualitative Research Methods: A Theoretical Perspective for Young Researchers," International Journal of Research, (February), pp. 70–87.
[10] Hossin, A., Du, J., Mu, L., and Asante, I. O., 2025, "Big Data-Driven Public Policy Decisions: Transformation Toward Smart Governance," , pp. 1–19.
[11] Stapleton, J. and Epstein, W. C., 2024, "Security Considerations," *Security Without Obscurity*, pp. 155–176.
[12] Sanabia-Lizarraga, K. G., Carballo-Mend, B., Arellano-Gonz, A., and Bueno-Solano, A., 2024, "Business Intelligence for Agricultural Foreign Trade: Design and Application of Power BI Dashboard," Sustainability.
[13] Shaikh, F. A. and Siponen, M., 2023, "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to," Computers & Security, **124**, p. 102974.
[14] Kaur, S., Singh, J., and Ghumman, N. S., 2014, "Network Programmability Using POX Controller," *International Conference on Communication and Computing Systems*, Paper No. August, p. 5.
[15] ENISA, 2018, "ENISA Threat Landscape Report 2017," EU Law and Publications, Tech. Rep. January.