IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Check for updates

Assessing the impact of cybersecurity incidents on financial losses and user exposure in the global financial sector (2015-2024)

Abdul-waliyyu Bello [1, *], Idris Wonuola [1], Callistus Obunadike [1], Anastesia Izundu [2] and Jacinta Izundu [3]

[1] *Department of Mathematics and Statistics, Austin Peay State University, Tennessee, USA.*
[2] *Department of Public Health, University of Illinois at Springfield, Illinois, USA.*
[3] *Department of Cybersecurity Management, University of Illinois at Springfield, Illinois, USA.*

International Journal of Science and Research Archive, 2025, 16(01), 489-504

Publication history: Received on 29 May 2025; revised on 05 July 2025; accepted on 07 July 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2037

Abstract

This study investigates the impact of cybersecurity incidents on financial losses and user exposure in the global financial sector, analyzing data from 2015 to 2024. The study utilizes machine learning models, specifically Random Forest and XGBoost, to predict the extent of financial damage and the number of affected users based on various cybersecurity incident characteristics, including attack type, source, and resolution time. The findings indicate that XGBoost outperforms Random Forest, with higher predictive accuracy ($R^2 = 0.74$) and lower error metrics (RMSE = 14.52, MAE = 6.08). Key features influencing financial loss include Incident Resolution Time, Country, and Year, with Incident Resolution Time emerging as the most significant predictor. Phishing, social engineering, and DDoS attacks were identified as the most financially damaging, emphasizing the need for robust defense mechanisms. Feature importance analysis further revealed that defense mechanisms, particularly VPNs and AI-based detection, play critical roles in mitigating losses. Despite the strong performance of both models, the study highlights challenges such as class imbalance in the data, which affects minority class detection. Recommendations include investing in AI-driven detection systems, enhancing employee awareness, adopting multi-factor authentication, and updating legacy systems. These measures are crucial for reducing financial and reputational damage. The study concludes that machine learning techniques, particularly XGBoost, can significantly improve cybersecurity practices in the financial sector, providing accurate, real-time predictions that enhance risk management and defense strategies.

Keywords: Cybersecurity; Financial Loss; Machine Learning; Random Forest; XGBoost; Risk Management

1. Introduction

The financial sector is rapidly growing globally as a result of the digital transformation that took the world by storm. This has led to higher productivity, operational efficiency, with many actors in the financial industry scaling their businesses seamlessly, leading to customer convenience and satisfaction (Alsakini, Alawawdeh, & Alsayyed, 2024). Several technologies have been introduced, which enabled transitioning from conventional banking to adoption of digital banking, as well as trading on high frequency (Abdajabar & Md Yunus, 2023). Cloud computing and big data analytics are a few of the advanced technologies that has contributed to the growth of substantial organizations in the financial sector across the world. This is holding to the significant operational benefits they derive from these tools, which has seen companies across different industries also adopting digital technologies for scalability (Cremer, et al., 2022).

Undoubtedly, digital transformation came with a lot of benefits for the world, but its usefulness comes with some risks, considering that there are cybercriminals who are constantly looking for loopholes to steal valuable resources of these

[*] Corresponding author: Abdul-waliyyu Bello.

organizations (Calliess & Baumgarten, 2020). The financial sector remains one of the most targeted industries, given that it is highly dependent on digital technologies for its operation in modern times. According to (Shehab, et al., 2024), about 80% of banking transactions across the world were digital in 2022, which is a significant increase to 40% carried out in 2015. While this is a commendable improvement, it introduces multi-faceted cybersecuirty threats against data and financial systems security globally. Given this, cybersecuirty incidents in the financial sector cannot be viewed from the perspective of occasional disruption anymore, rather it should be perceived as threats that leave customers and financial organizations at a great risk as asserted by (Abdajabar & Md Yunus, 2023).

As reported by (Seh, et al., 2020), the average cost of a data breach in the financial industry is approximately $5.97 million, which is second to only the healthcare sector. Cyber criminals are known to adopt different attack vectors, particularly malware, phishing, distributed denial-of-service, and ransomware (Erkan-Barlow, Ngo, & Goel, 2023). The 2017 Equifax data breach, which exposed the personal data of 147 million individuals, serves as a stark reminder of the massive financial and reputational damage such attacks can cause. The frequency and sophistication of these threats have escalated rapidly, with cybersecurity breaches increasing by over 50% between 2015 and 2023 (Pollmeier, Bangiovanni, & Slapnicar, 2023).

Being the manager of high-value assets makes financial institutions one of the attractive targets of cybercriminals, usually based on the understanding that they are in possession of sensitive information for the company and depositors (Alsakini, Alawawdeh, & Alsayyed, 2024). Cyberattack motivations include financially motivated theft, corporate sabotage, and technically motivated geopolitical hot war (Bouveret, 2018). All of which have impact the financial services industry, especially when you consider the inherent interconnected nature of financial services, the reliance on third-party vendors in the ecosystem, increased opportunities for money laundering through counterfeit statements of account, unstable currencies that are notorious in hacktivist cyberspace (Razavi, Jamali, Emsaki, Ahmadi, & Hajiaghei-Keshteli, 2023). If a single organization in the ecosystem is hacked, as in the case of Cloudflare, all of their customers are compromised (Aldasoro, Gambacorta, Giudici, & Leach, 2023).

Apart from the financial loss consequences of cyberattacks, it is also associated with loss of user trust and regulatory compliance challenges (Shaddad, 2023). It leaves users highly vulnerable to identity theft, fraud, and non-consented transactions, which may worsen the trust in the digital banking and reduction in the use of such services. As reported by (Jimmy, 2024), 58% of financial service consumers reported concerns about the safety of their personal data online, and 34% considered switching providers following a data breach. This erosion of user trust has prompted regulators to introduce stricter compliance mandates, including the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, which impose heavy penalties on institutions that fail to protect consumer data (Erkan-Barlow, Ngo, & Goel, 2023).

Despite these regulatory successes and ramping up investment in cybersecurity, estimated globally at $187 billion in 2024 (Alsakini, Alawawdeh, & Alsayyed, 2024), readiness and resilience gaps remain. Most financial institutions cannot adapt to evolving threats due to legacy infrastructure, restricted availability of cybersecurity professionals, and uneven best practice application (Lagarde, 2018). Furthermore, the absence of standardized global reporting and response systems to cyber-attacks disables synergistic defense effort and weakens institutional response (Aldasoro, Frost, Gambacorta, Leach, & Whyte, 2020). Thus, a close examination of how cyber breaches impact financial losses and user exposure by region and over time is timely and justified. That is what this paper attempt to accomplish by presenting an in-depth empirically based analysis of global financial sector cybersecurity trends from 2015 through 2024.

2. Literature review

2.1. Cybersecurity and Associated Incidents

Cybersecurity has emerged as a cornerstone of modern financial infrastructure, underpinning the integrity, confidentiality, and availability of digital assets and services. (Wang, Nnaji, & Jung, 2018) defined as the practice of protecting systems, networks, and data from digital attacks, cybersecurity has grown in complexity due to the increasing integration of financial services with digital technologies. Academic interest in the field has expanded significantly over the past decade, reflecting the sector's heightened vulnerability to cyber threats. (Bouveret, 2018) found that organizations with proactive risk management cultures tend to allocate more resources to cybersecurity infrastructure and experience fewer breaches. Similarly, (Razavi, Jamali, Emsaki, Ahmadi, & Hajiaghei-Keshteli, 2023) established that financial institutions with well-developed IT governance structures demonstrated significantly higher levels of cyber resilience. The implication of this is that beyond technological tools, institutional norms and internal control environments play a critical role in mitigating cyber risks.

(Cremer, et al., 2022) demonstrated that mandatory disclosure laws positively impact firms' willingness to invest in cybersecurity, as transparency increases reputational risk for non-compliance. From the perspective of (Luque, Lopez, & Williams, 2021), there is a significant relationship between compliance-driven investments in cybersecurity and reductions in the likelihood of data breaches. However, cybersecurity remains unevenly prioritized across regions and organizations. (Jin, Li, Liu, & Khalid Nainar, 2023) underscore that in many emerging economies, cybersecurity frameworks remain underdeveloped, with low levels of institutional capacity to manage sophisticated attacks.

A cybersecurity incident is any real or attempted unauthorized access, disruption, or use of an information system (Abdajabar & Md Yunus, 2023). Financial institutions, in the view of (Calliess & Baumgarten, 2020), are more vulnerable due to the type of data they handle and the potential for direct financial benefit. Cybersecurity breaches range from malware to insider attacks with varying severity and recovery costs. (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024) acknowledge that organizations with incident response plans spend less on recovery and experience shorter recovery times. Moreover, incidents cause chain reactions within systems, especially financial networks that are interconnected.

2.2. Data Breach

A data breach is an unauthorized acquisition or disclosure of confidential data, which often includes personal or financial data. The number of data breaches and their severity has increased over the last decade, particularly in the finance sector (Alsakini, Alawawdeh, & Alsayyed, 2024). (Seh, et al., 2020) found that institutions that maintain large datasets may be more likely to suffer a data breach, and data breaches that involve financial data tend to have more severe consequences. Also keep in mind that the type of breached data, such as a social security number and email address, may lead to different outcomes, such as litigation or regulatory fines. (Jooda, Aghaunor, Kassie, & Oyirinnaya, 2023) identified weak access controls and software that is not up-to-date as major enabling factors. There is general agreement that data breaches are increasing and adopting data minimization and encryption-at-rest can decrease the impact if a data breach were to occur.

2.3. Financial Loss

Economic damage resulting from cybersecurity incidents includes direct cost, fraud, remediation, and legal fees, and indirect harm in the way of reputational damage and customer loss (Luque, Lopez, & Williams, 2021). Statistical drops in stock price and increased volatility are a consequence of data breaches and cyberattacks against financial institutions, as (Wang, Nnaji, & Jung, 2018) reported. (Skinner, 2019) reports that the average data breach cost in the financial sector is $5.72 million, higher than in most other sectors. (Aldasoro, Gambacorta, Giudici, & Leach, 2023) argued that losses are magnified when institutions procrastinate disclosure or are underinsured. Losses are also not evenly spread; small institutions have proportionally higher losses due to their limited resources and response capability (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024). This implies that financial institution needs to invest in proactive cyber defense, which is achievable through predictive financial modelling, an ideal strategy to mitigate costs.

2.4. User Exposure

User exposure is a cyber-security term which describes, the degree of possibility a user has in allowing their stolen personal information, their stolen identity, or their service being interrupted by security violation (Cremer, et al., 2022). User exposure increases when financial services do not have strong encryption, multi-factor authentication and user awareness (Lagarde, 2018). (Ibrahimnur, 2023) collate evidence on breach events but further contend that many breach events entail the downstream effect on the personal identity use, over a timeframe that can erode the consumer confidence in financial services going forward. Second, user exposure tends to track regulatory loopholes, where jurisdictions with less developed data protection regulation present more exposure (Shehab, et al., 2024). The Equifax and Capital One event occurrences represent the long-term consequences of inadequate data governance on user safety and exposure. Therefore, researchers are urging situation-aware, user-oriented security models that would be agreeable to user knowledge of their data through transparency, immediate breach notification, with the ability to opt-out (Jimmy, 2024).

2.5. Threat Vectors

In recent years, cybersecurity research has increasingly focused on understanding the role of threat vectors in shaping the scale and impact of cyber incidents, particularly within the financial sector (Abdajabar & Md Yunus, 2023). Threat vectors represent the routes through which attackers penetrate systems, and they significantly determine both the likelihood of a breach and the extent of financial or user-level harm. (Luque, Lopez, & Williams, 2021) emphasize that the sophistication of attack vectors has evolved alongside advancements in technology, making conventional security measures less effective against emerging forms of exploitation. These threats include:

2.5.1. Ransomware

Ransomware is malicious software that encrypts information or systems, after which attackers request payment in return for decryption keys. In studies concerning ransomware, studies show a dramatic increase in attacks against the financial sector, attributing their employment of the consistency of data and availability (Pollmeier, Bangiovanni, & Slapnicar, 2023). Ransomware attacks have evolved from indiscriminate scattershot attack models to organized campaigns. (Wang, Nnaji, & Jung, 2018) cited that while some ransomware orchestrators start with a scattershot approach, they later zeroed in on organizations that are relevant to their specific business. These attacks are largely exploited via phishing, or exploitation of Remote Desktop Protocol (RDP) access of a victim machine. In academic literature, paying the ransom is not a return to the original system, and may confer some sort of prestige upon attackers due to the fact that their funds were breached successfully (Skinner, 2019). Examples of the cost in money of ransomware include not just the ransom, but any downtime of operations, loss of data, and reputational damage as well. With increased ransomware prevalence, regulatory agencies recommend against paying the ransom since in their stead, they recommend stronger backup procedures, incident reporting plans, and employee training (Maheswari, Chaudhary, Manna, Khalane, & Muthukumar, 2024).

2.5.2. Phishing

Phishing is a form of simulation where one pretends to be a form of communication, most frequently emails or messages, that are designed to deceive recipients into revealing sensitive information, or into downloading malware. It is still one of the most common and effective methods of launching a cyberattack (Alsakini, Alawawdeh, & Alsayyed, 2024). (Alkhdour, et al., 2024) showed that phishing works so often due to human factors such as stress, fatigue, or ignorance of potential digital risks. Within the financial community, phishing is most commonly directed at acquiring credentials employed to log in to accounts or networks within. (Calliess & Baumgarten, 2020) proved that phishing constitutes over 70% of cyber intrusions in the banking infrastructure. Consequently, there has been a surge in behavioral cybersecurity research, attempting to understand user vulnerability and provide anti-phishing training to users. Multi-factor authentication, and computer-driven e-mail filters have strongly been recommended as a counter-measure against the threat of phishing (Jooda, Aghaunor, Kassie, & Oyirinnaya, 2023).

2.5.3. Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks continue to be a bane of the financial sector when it comes to disruption of service availability. (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024) claims that the DDoS recovery times are among the highest by financial institutions; coming back from paralysis of operations by an organization and ensuing reputation loss. Observe that DDoS attacks are heavily misconceived since they do not even directly breach data, they cripple it by overwhelming services. They take advantage of bandwidth depletion and resource depletion. Even though DDoS attacks do not compromise the data, they indirectly cause loss of customer confidence, time lag in operations, and increased incident response cost (Shehab, et al., 2024). The three-step approach to counter DDoS is via firewalls and load balancers, but they are not sufficient against large-scale or multi-vector DDoS. With DDoS-as-a-Service, barriers to entry have dropped significantly for attackers. This comes on top of greater use of DDoS as a smokescreen for data exfiltration and other attacks. DDoS attacks appear to be shifting towards more sophisticated, coordinated cybercrime, rather than just service disruption (Jin, Li, Liu, & Khalid Nainar, 2023).

2.5.4. SQL Injection Attacks

SQL injection remains a highly exploited web-based financial system weakness and frequently results in unauthorized database access with confidential customer information. (Maheswari, Chaudhary, Manna, Khalane, & Muthukumar, 2024) show that SQL injection is frequently encountered in the scopes of inadequately sanitized user input such as in login screens, search screens, or finance consoles. In the financial industry, where information integrity and confidentiality are paramount, SQL injection might result in siphoning of funds or services, direct record altering, or even outright hijacking of the system's administrative control. Although (Erkan-Barlow, Ngo, & Goel, 2023) continues to include it among the most critical threats to web systems, and although there is general awareness within financial institutions of the issue, the reality that it remains one of the most exploited vulnerabilities demonstrates that there is a disconnect between security awareness and security practice. The safeguards incorporated into existing frameworks (parameterized queries directly and ORM) are hard to apply correctly consistently but there is usage and adaptation of legacy systems and smaller financial institutions that do not appear to have the necessary rigor (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024). The barrier to entry to prevent exploitation in SQL is low, i.e., SQL injection has become a threat within both high- and low-value financial institutions.

2.5.5. Man-in-the-Middle (MitM) Attacks

Man-in-the-middle attacks are an unnoticed but severe problem for the entire financial sector, particularly in low encryption network settings or when adequate user authentication is in jeopardy. (Bouveret, 2018) indicates that MitM attacks occur most commonly on unsecured or public networks, thus allowing the attacker to capture credentials, financial transactions or API tokens. While HTTPS and VPNs can lessen exposure, there are still cases of MitM attacks especially when older TLS versions or a self-signed certificate is used (Pollmeier, Bangiovanni, & Slapnicar, 2023). Specifically, MitM attacks are not detected until the fraud incident occurs because they are stealth in nature in terms of implementation. Attackers will use social engineering, phishing, or a malicious program to place themselves between the user and the service but still pass through or modify communication from either presentation (Wang, Nnaji, & Jung, 2018). In financial terms, most significantly, this could be performed upon a financial transaction or bank session online and would allow only money or access through sessions to be carried out without authorization. The attack is exploiting human and infrastructure weaknesses, highlighting the need for an approach of a security nature with multiple layers being put in place (Lagarde, 2018).

2.6. Overview of Cybersecurity Threats in the Financial Sector

Enemies continuously exploit ransomware, phishing, insider compromises, denial of service attacks, and other evolving threats that are not showing any sign of diminishing their sophistication or frequency and have global reach (Alkhdour, et al., 2024). Impacts suffered are in terms of financial losses directly, loss of reputation, regulatory action, and loss of customer confidence. Ransomware is still perhaps the costliest threat to financial services (Cremer, et al., 2022). The attackers conducting a ransomware attack can not only encrypt and shutdown critical systems or data, but also extort a payment in the process. Financial institutions are particularly at risk due to operational pressures of time-sensitive services (Luque, Lopez, & Williams, 2021). Ransomware strains like Maze and LockBit included "double extortion" in the form of not only denying them access to the systems but also threatening to release sensitive data if payment was not made (Jimmy, 2024). The losses can be immense, from ransom payments, data breaches, to business continuity.

Phishing remains an early large attack vector. Phishing attacks are familiar to users, and user education programs exist everywhere; Phishing has instead turned into spear-phishing and business email compromise (BEC), which are more focused. Based on the Verizon Data Breach Investigations Report (2023), since the start of the pandemic, more than 80% of the financial sector's breaches began through phishing. Phishing is usually used to gain credentials, obtain initial access, or deliver a malware payload, and then the cycle repeats, usually leading to account compromise, wire fraud, or unauthorized data access. Insider threats, both willing and inadvertent, present unique challenges to the financial sector (Seh, et al., 2020). Insider breaches are hard to detect as insiders have legitimate access to sensitive systems. When insider knowledge comes in the form of an upset employee disclosing sensitive information or employees accidentally exposing the system through phishing links or poor passwords, insider breaches can be as harmful as breaches from outside. The (Center, 2021) describes that incidents involving insiders in financial institutions occur more often than in many other industries and thus information security directors must ensure system monitoring and access controls are bolstered.

Over the past decade, attacks have progressed from stand-alone data breaches to more sophisticated, multi-phase attacks. Phishing attacks are most commonly used today in combination with credential theft and privilege escalation and lateral movement within networks (Razavi, Jamali, Emsaki, Ahmadi, & Hajiaghei-Keshteli, 2023). Blended threats have been shown to be extremely powerful-mostly against legacy systems and under-patched environments. The 2019 Capital One breach exposed the private information of more than 100 million individuals, indicating the use of a misconfigured firewall being exploited (Aldasoro, Frost, Gambacorta, Leach, & Whyte, 2020). That demonstrates how easy security mistakes can lead to huge breaches. The case of the Equifax breach in 2017 resulted from a patch not being applied to a known Apache Struts vulnerability, exposing the records of 147 million Americans and eliciting a $700 million settlement (Maheswari, Chaudhary, Manna, Khalane, & Muthukumar, 2024). More recently, threat actors have increasingly employed zero-day exploits and supply chain breaches to access financial networks. The 2020 SolarWinds attack, though not targeting the financial sector alone, sparked global concern over the threat from third-party software (Jooda, Aghaunor, Kassie, & Oyirinnaya, 2023). In response, institutions began adopting more multi-layered and intelligence-driven defense measures, such as AI-driven threat detection, behavioral inspection, and zero-trust frameworks.

2.7. Factors Influencing Financial Loss and Exposure

Among the most important aspects of loss is the exploit library, although what is important is known vulnerability use. Not surprisingly, unpatched software vulnerabilities continue to be one of the most common types of violation (Abdajabar & Md Yunus, 2023). The high-profile Equifax (2017) and Capital One (2019) data breach, whose occurrence was confirmed to have occurred due to publicly patched vulnerabilities, or publicly available patches, is one such example (Alsakini, Alawawdeh, & Alsayyed, 2024). Attackers can increase dwell times for data exfiltration, or system compromise, through their attacks on unpatched systems (Verizon DBIR, 2023). Weak passwords, or rightfully poor authentication means, still persist in numerous customer-facing software like online banking apps.

The use of passwords as system protection may be worsened by the replacement of weak passwords with multi-factor authentication (MFA) that exposes customers to credential stuffing or brute-force attacks that lead to eventual account takeover and fraud transactions (Calliess & Baumgarten, 2020). They are the least common but most expensive of all vulnerabilities in the list, once more there is no patch for a zero-day exploit while it is currently being exploited. Zero-day exploits are usually employed in directed attacks, or, in financial systems based on prevalent current popular financial systems, to maintain target marketing resulting in even greater information loss and ultimate cost of such breaches (Pollmeier, Bangiovanni, & Slapnicar, 2023). Either that or through account takeover, user bank investigation penalty, and regulatory abuse penalties.

Another reason behind this is the risk exposure of various financial sub-industries. Banks and payment processors have a bullseye on them back due to the immediacy of money that is associated with their assets (Lagarde, 2018). Insurers may not have cash as custodians, but they certainly have a treasure trove of personally identifiable information (PII) and financial information that is very attractive to a broad spectrum of attackers and can be used to commit a broad spectrum of identity thefts or financial breaches (Aldasoro, Gambacorta, Giudici, & Leach, 2023). Smaller financial institutions, such as credit unions or fintech companies, may be at risk because they possess limited funds to spend on cybersecurity and few risk governances that has been established. (Ibrahimnur, 2023) reveals that even though larger banks are vulnerable to more advanced persistent threats, losses made by smaller institutions relative to their size are much higher since they possess minimal recovery capacity and protections. In addition, the defensive control maturity is an important catalyst of financial and data exposure outcomes.

Legacy controls such as firewalls and antivirus have their capabilities diminished to the point that they are now just a single value of protection (Abdajabar & Md Yunus, 2023). Today, there are a vast array of new technologies to learn day by day - AI-driven deployment threat detection technologies, endpoint detection and response (EDR) and, behavior analytics technology, among many others, which work together to enable the automation of anomaly detection and negatively compress effective response time. (Jin, Li, Liu, & Khalid Nainar, 2023) identified that the organizations that adopt AI-powered security solutions have a 27% lower chance of the average breach cost when compared to the adoption of legacy security controls. VPNs are ubiquitous but are most often a leading cause of credential theft.

Incident response speed is an essential component of damage control. The quicker a breach is found and dealt with, the less expensive it will be monetarily and for reputation. (Bouveret, 2018) shows that businesses that contained an incident in 30 days saved a mean of over $1 million compared to slow-response organizations. Fast containment minimizes data theft, halts system disruption, and minimizes customer churn. Yet, many financial institutions do not yet have real-time monitoring or automated incident response capabilities, increasing exposure time.

2.8. Theoretical review

This study is underpinned by the Risk Management Theory, which provides a structured framework for identifying, analyzing, and mitigating risks that threaten the financial performance and operational integrity of organizations. From cybersecurity perspective, this theory emphasizes the assessment of potential vulnerabilities and threats, the likelihood of their occurrence, and the quantifiable consequences, such as financial loss and user exposure, if left unmanaged. Within the financial sector, risk management theory is especially relevant due to the industry's exposure to complex and evolving cyber threats (Oyewole, Okoye, Ofodile, & Ugochukwu, 2024). Financial institutions operate in a high-risk environment where data confidentiality, system availability, and transactional integrity are critical. As outlined by (Shaddad, 2023), effective risk management requires not only identifying threats like phishing, DDoS, or insider attacks but also evaluating their impact on both financial metrics and customer trust.

This theoretical lens supports the study's focus on empirical relationships between the nature of cybersecurity incidents and their resultant losses. It also highlights the importance of organizational preparedness, including security architecture, response time, and defense mechanisms (Jimmy, 2024). By framing cybersecurity incidents as quantifiable operational risks, Risk Management Theory allows the study to analyze how different threat vectors, defense strategies, and sector-specific vulnerabilities contribute to financial damage and data compromise. The theory provides justification for integrating machine learning techniques into impact prediction, aligning with the risk principle of using historical data to forecast and mitigate future losses. Ultimately, Risk Management Theory offers a practical and analytical basis for this study's investigation into minimizing the operational and reputational risks posed by cyberattacks in the financial domain (Skinner, 2019).

2.9. Gaps in the Reviewed Literature

While several studies have explored cybersecurity threats in the financial sector, few have systematically linked specific threat vectors to both financial loss and user exposure. Most existing research focuses either on the technical classification of attacks or on data breaches in isolation, often overlooking the dual impact on economic performance and customer trust. Additionally, prior literature tends to be geographically concentrated on developed economies, leaving limited insight into how cybersecurity incidents affect financial institutions across diverse global contexts, particularly in emerging markets where digital infrastructure and incident response capacity may be weaker.

Additionally, response time and defense mechanisms are frequently mentioned but rarely analyzed as explanatory variables for the extent of damage. The role of delayed resolution in escalating financial loss or user compromise remains empirically underexplored. Finally, despite the increasing availability of cyber incident datasets, the application of machine learning techniques to predict loss severity or exposure risk is still limited in academic studies. These gaps highlight the need for a more integrated, data-driven approach to understanding the financial and operational consequences of cyberattacks in the financial sector.

3. Methodology

3.1. Research Design

This study adopts a quantitative, predictive research design to examine the relationship between cybersecurity incidents and their impact on financial loss and user exposure within the global financial sector from 2015 to 2024. The approach leverages supervised machine learning techniques to develop regression models that estimate the extent of financial damage and number of affected users based on incident-level characteristics.

The design is structured around secondary data analysis using a labeled dataset of cybersecurity breaches. Given the numerical nature of the outcome variables and the presence of both categorical and continuous predictors, the study employs machine learning algorithms capable of handling high-dimensional, mixed-type data. This allows for better pattern recognition and predictive accuracy than traditional statistical models.

3.2. Data Source and Scope

The dataset used in this study was obtained from Kaggle, a public data platform known for curated datasets across diverse domains. The dataset contains detailed records of global cybersecurity incidents between 2015 and 2024. For the purpose of this study, the data was filtered to include only incidents affecting the financial sector. Each row represents a unique cybersecurity event with attributes such as country, year, attack type, source of attack, vulnerability exploited, defense mechanism used, incident resolution time (in hours), financial loss (in USD millions), and the number of affected users.

The dataset spans multiple countries and attack categories, providing sufficient variability for machine learning analysis. Only complete records were used to ensure data integrity during modeling. The structured nature of the dataset makes it suitable for supervised learning tasks focused on predicting financial losses and user exposure resulting from cyber threats within the financial sector.

3.3. Variables and Measurement

This study focuses on two main outcome variables: Financial Loss and Number of Affected Users, both treated as continuous variables. These serve as the target variables for the machine learning regression models.

The predictor variables (feature vector) include a mix of categorical and numerical fields. Country, Attack Type, Attack Source, Security Vulnerability Type, and Defense Mechanism Used are all categorical variables that describe the nature and context of each cybersecurity incident. Year is treated as a numerical variable to account for potential time-based trends, while Incident Resolution Time is a continuous numerical variable measured in hours. Only observations from the financial sector were retained, as specified in the Target Industry column. Categorical features will be encoded using appropriate transformation techniques, such as one-hot encoding or label encoding, to prepare the data for machine learning algorithms.

3.4. Analytical Techniques

The study employs supervised machine learning techniques to model the relationship between cyber incident features and their outcomes in terms of financial loss and user exposure. After preprocessing the dataset, handling missing values, encoding categorical variables, and normalizing continuous features, separate regression models will be developed for each target variable.

Three algorithms will be implemented for comparison: Linear Regression (as a baseline), Random Forest Regressor, and XGBoost Regressor. These models were selected for their ability to handle both numerical and categorical inputs and capture non-linear relationships. Model performance will be evaluated using R-squared (R^2), Root Mean Square Error (RMSE), and Mean Absolute Error (MAE). K-fold cross-validation will be applied to ensure the robustness and generalizability of results. The final models will be interpreted using feature importance scores to highlight the most influential predictors of financial loss and user impact.

3.5. Model Specification

This study develops two distinct supervised machine learning regression models

- Model 1: Predicting Financial Loss (in USD millions)
- Model 2: Predicting Number of Affected Users

Input Features (Independent Variables)

The models share the same feature set

Country; Year; Attack Type; Attack Source; Security Vulnerability Type; Defense Mechanism Used; Incident Resolution Time

While the target variables are

Y1: Financial Loss; Y2: Number of Affected Users

Each model is structured as follows:

$$Y_1 = f(X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8)$$

Where

Y_1 is the predicted outcome (either financial loss or user exposure)
f is the function learned by the ML algorithm
X_1 to X_8 are the transformed feature inputs

3.6. Preprocessing Steps

Categorical variables will be one-hot encoded to convert them into numerical format. Numerical variables like Year and Incident Resolution Time will be standardized when required by the algorithm. The dataset will be split into training (80%) and testing (20%) sets.

3.7. Modeling Algorithms

Baseline: Linear Regression

Primary Models: Random Forest Regressor, XGBoost Regressor

Models will be tuned using grid search or randomized search for optimal hyperparameters. This specification enables the models to predict the scale of damage resulting from cybersecurity incidents in the financial sector, based on structured historical features.

4. Results

Table 1 Descriptive Statistics for Key Variables (N = 890)

Variable	**Mean**	**Std. Dev.**
Financial Loss (in million $)	51.17	28.93
Number of Affected Users	505,839.11	302,183.90
Incident Resolution Time (hrs)	35.74	19.89

As shown in Table 1, the average financial loss from cybersecurity incidents in the financial sector was $51.17 million (SD = 28.93), with an average of 505,839 affected users (SD = 302,183.90). Incident resolution took an average of 35.74 hours (SD = 19.89). These results highlight the substantial financial and operational impact of cyberattacks, suggesting that incidents typically involve large user exposure and extended resolution times, which may contribute significantly to the overall cost and reputational risk.

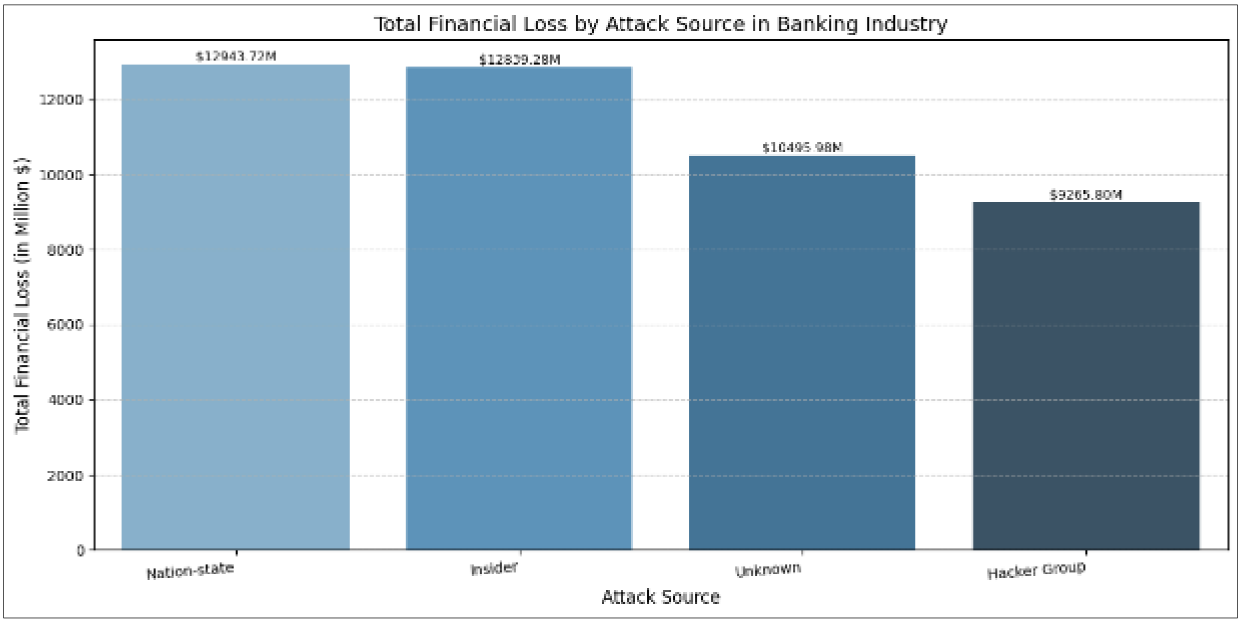

Figure 1 Financial Impact of Cyberattack Sources in the Banking Sector (2015–2024)

For Figure 1: Total Financial Loss by Attack Source in Banking Industry, the chart reveals the total financial losses attributed to various attack sources in the banking sector. Nation-state actors are the most financially impactful, causing a loss of $12943.72 million, closely followed by insider threats with a loss of $12839.28 million. Attacks attributed to unknown sources amounted to $10495.98 million, while hacker groups caused the least damage, with a total loss of $9265.80 million. These figures underline the significant financial consequences of both state-sponsored and insider cyberattacks within the financial industry.

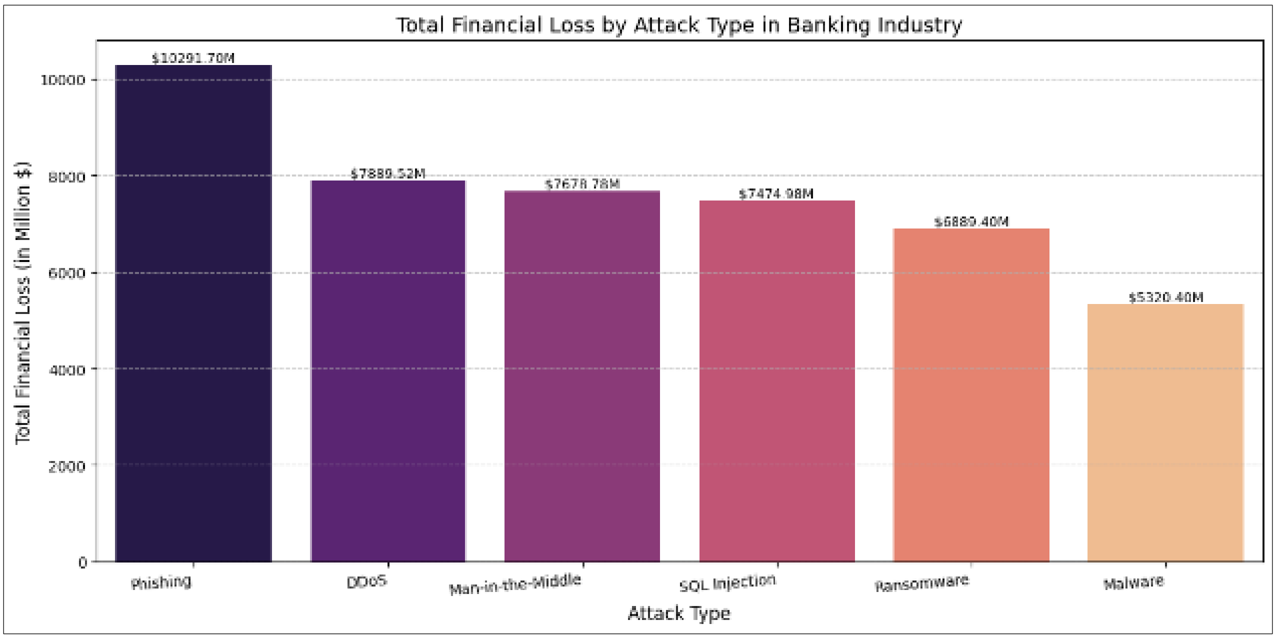

Figure 2 Comparative Financial Losses by Cyberattack Type in the Banking Sector (2015–2024)

For Figure 2: Total Financial Loss by Attack Type in Banking Industry, the chart demonstrates the financial impact of various cyberattack types within the banking industry. Phishing leads to the highest total loss at $10291.70 million, followed by Distributed Denial-of-Service (DDoS) attacks at $7889.52 million. Man-in-the-middle attacks and SQL injection incidents caused losses of $7678.78 million and $7474.98 million, respectively. Ransomware attacks, while significant, led to a loss of $6889.40 million. Malware, on the other hand, was the least costly in terms of financial impact, amounting to $5320.40 million. These findings highlight phishing as the costliest cyberattack type for financial institutions.

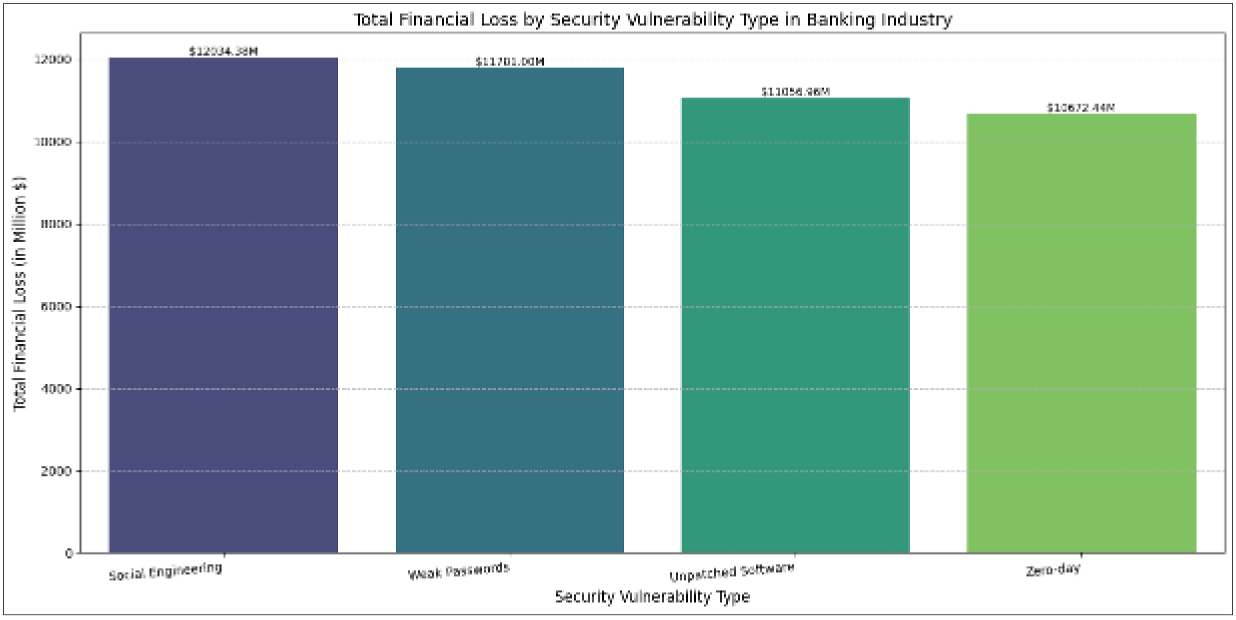

Figure 3 Total Financial Loss by Security Vulnerability Type in the Banking Industry (2015–2024)

For Figure 3: Total Financial Loss by Security Vulnerability Type in Banking Industry, the chart illustrates the financial losses associated with different types of security vulnerabilities in the banking sector. Social engineering emerged as the most financially damaging vulnerability, with a total loss of $12034.38 million. Weak passwords followed closely at $11781.00 million, showing the significant impact of inadequate security practices. Vulnerabilities associated with unpatched software and zero-day exploits resulted in slightly lower losses, at $11056.96 million and $10672.44 million, respectively. These figures emphasize the critical role of addressing both human and technological security flaws in financial institutions.

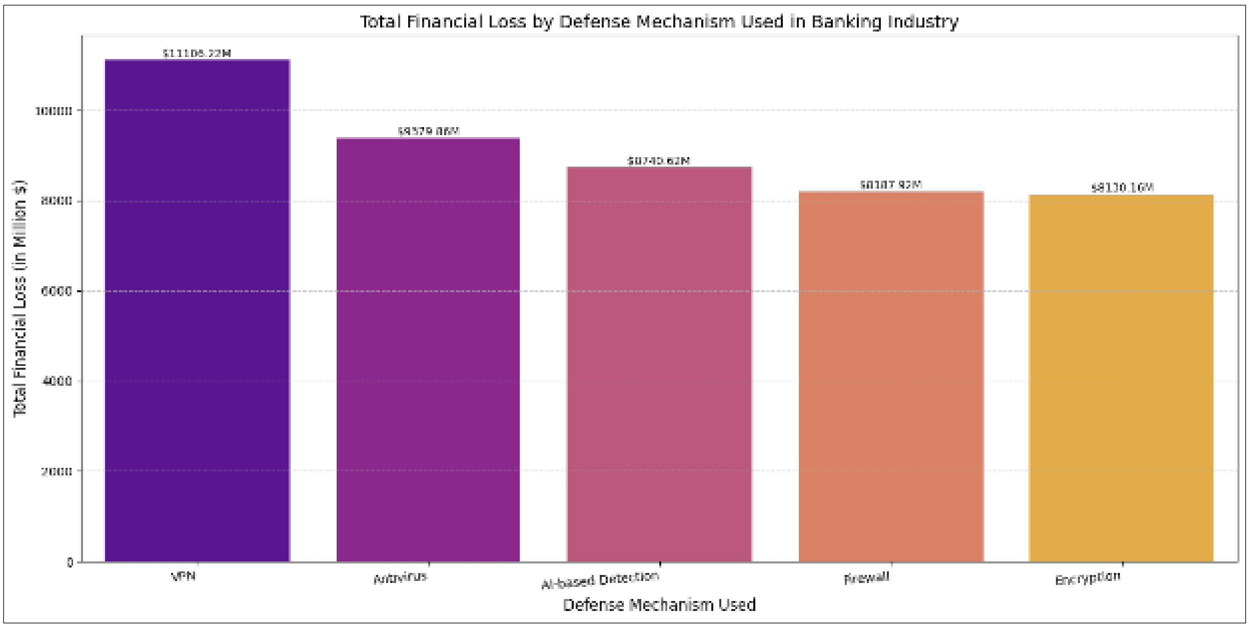

Figure 4 Financial Losses Associated with Defense Mechanisms in the Banking Sector (2015–2024)

For Figure 4: Total Financial Loss by Defense Mechanism Used in Banking Industry, the chart compares the total financial losses (in millions of dollars) associated with different defense mechanisms employed in the banking industry. VPNs, despite being a common defense, were linked to the highest total financial loss of $11106.22 million. Antivirus solutions followed closely with a total loss of $9379.86 million. AI-based detection systems and firewalls reported losses of $8740.62 million and $8187.92 million, respectively. Encryption tools, while critical, had the lowest associated loss at $8130.16 million, indicating varying effectiveness across defense strategies.

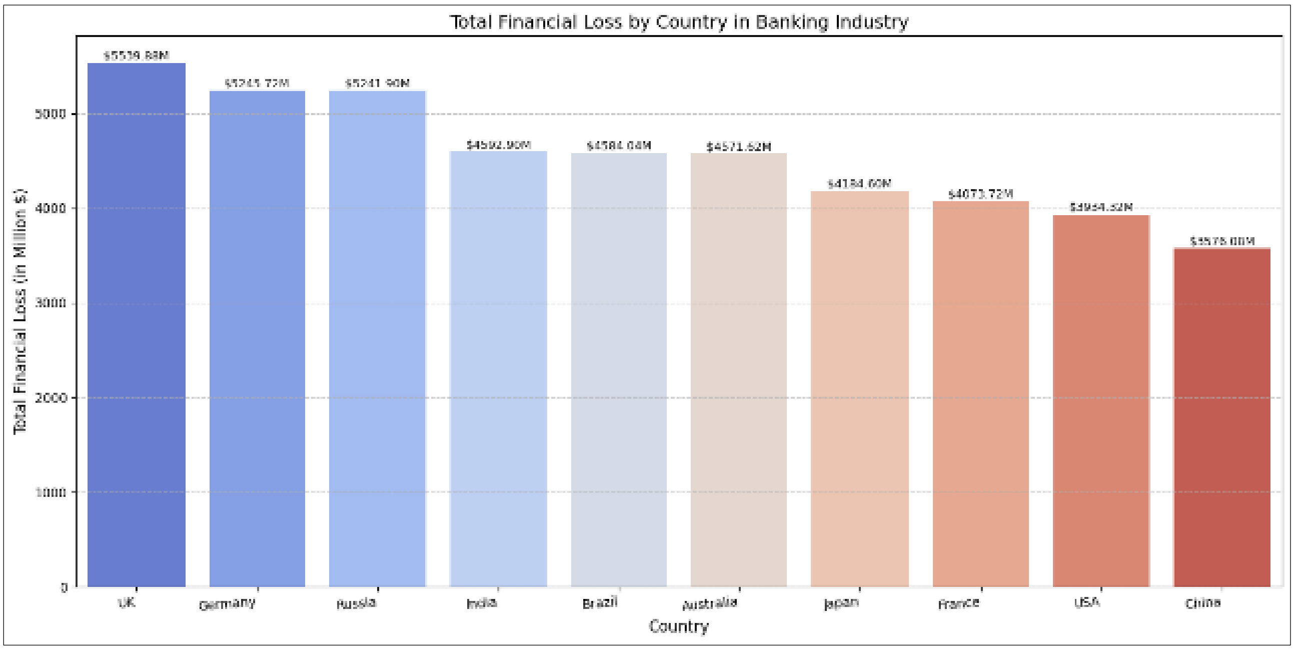

Figure 5 Geographic Distribution of Financial Losses from Cyberattacks in the Banking Industry (2015–2024)

For Figure 5: Total Financial Loss by Country in Banking Industry, the data shows the financial loss in millions of dollars resulting from cyberattacks across different countries in the banking industry. The UK experienced the highest total financial loss at $5539.88 million, followed by Germany ($5245.72 million) and Russia ($5241.90 million). Other countries like India, Brazil, and Australia reported losses ranging from $4571.62 million to $4629.90 million. In contrast, China had the lowest total financial loss among the countries listed at $3576.08 million. This chart highlights the impact of cybersecurity threats and their varying severity across geopolitical regions.

5. Model performance

Table 2 Model Performance for Predicting Financial Loss and User Exposure

Model	**Outcome**	**R^2**	**RMSE**	**MAE**
Linear Regression	Financial Loss	-0.04	29.12	25.07
Random Forest	Financial Loss	0.66	16.73	12.84
XGBoost	Financial Loss	0.74	14.52	6.08
Linear Regression	User’s Exposure	0.02	257203.56	295149.26
Random Forest	User’s Exposure	0.61	139153.04	186281.66
XGBoost	User’s Exposure	0.68	74137.28	168618.64

As shown in Table 2, the linear regression models served as baseline models and demonstrated limited predictive ability for both financial loss (R^2 = –.04) and user exposure (R^2 = .02). In contrast, the XGBoost models achieved the best performance across both outcomes. For financial loss, XGBoost produced the highest predictive accuracy (R^2 = .74), with the lowest RMSE (14.52) and MAE (6.08). Similarly, for user exposure, XGBoost outperformed the others (R^2 = .68), indicating its superior capability in capturing complex, non-linear relationships in the data.

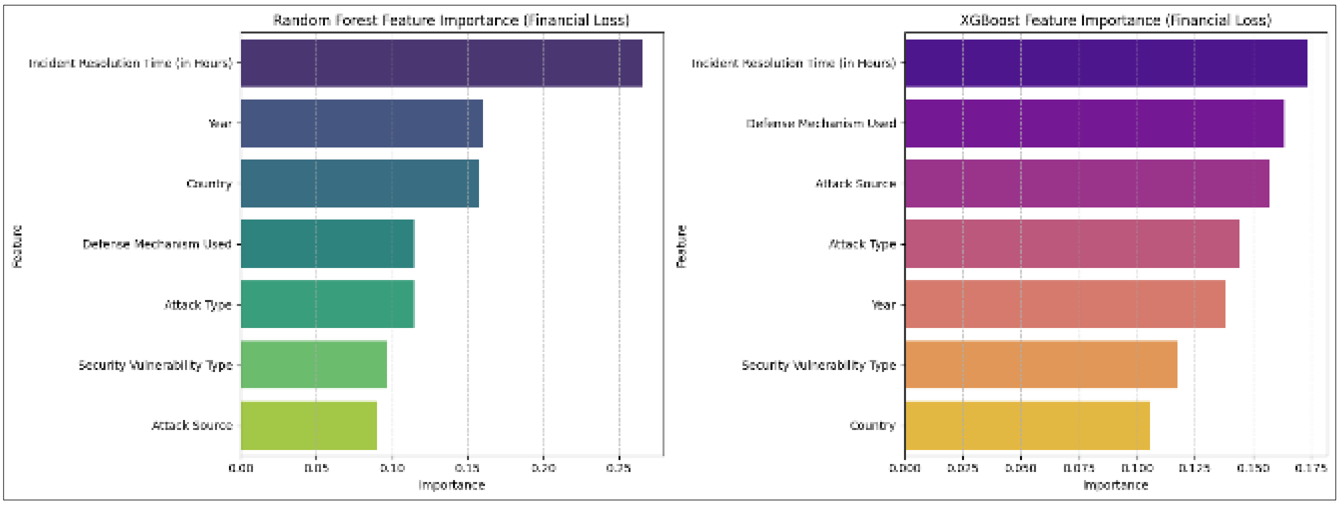

Figure 6 Feature Importance Comparison for Predicting Financial Loss: Random Forest vs. XGBoost Models

The results of the feature importance for both Random Forest and XGBoost models in predicting financial loss highlight the key factors driving their predictions. For Random Forest, the most significant feature is Incident Resolution Time in Hours, indicating that the duration it takes to resolve an incident is a critical determinant of financial loss. Following this, Year and Country also hold substantial importance, suggesting that temporal and geographical factors influence financial loss in a meaningful way. Defense Mechanism Used, Attack Type, Security Vulnerability Type, and Attack Source are ranked lower, showing that while they have some impact, they are less influential in determining financial loss. In XGBoost, Incident Resolution Time remains the most important feature, confirming its pivotal role. Defense Mechanism Used and Attack Source are ranked highly, emphasizing that the types of defenses in place and the origin of the attacks are more critical in this model. Attack Type, Year, Security Vulnerability Type, and Country follow in decreasing order of importance, reflecting their lesser but still relevant contribution to predicting financial loss.

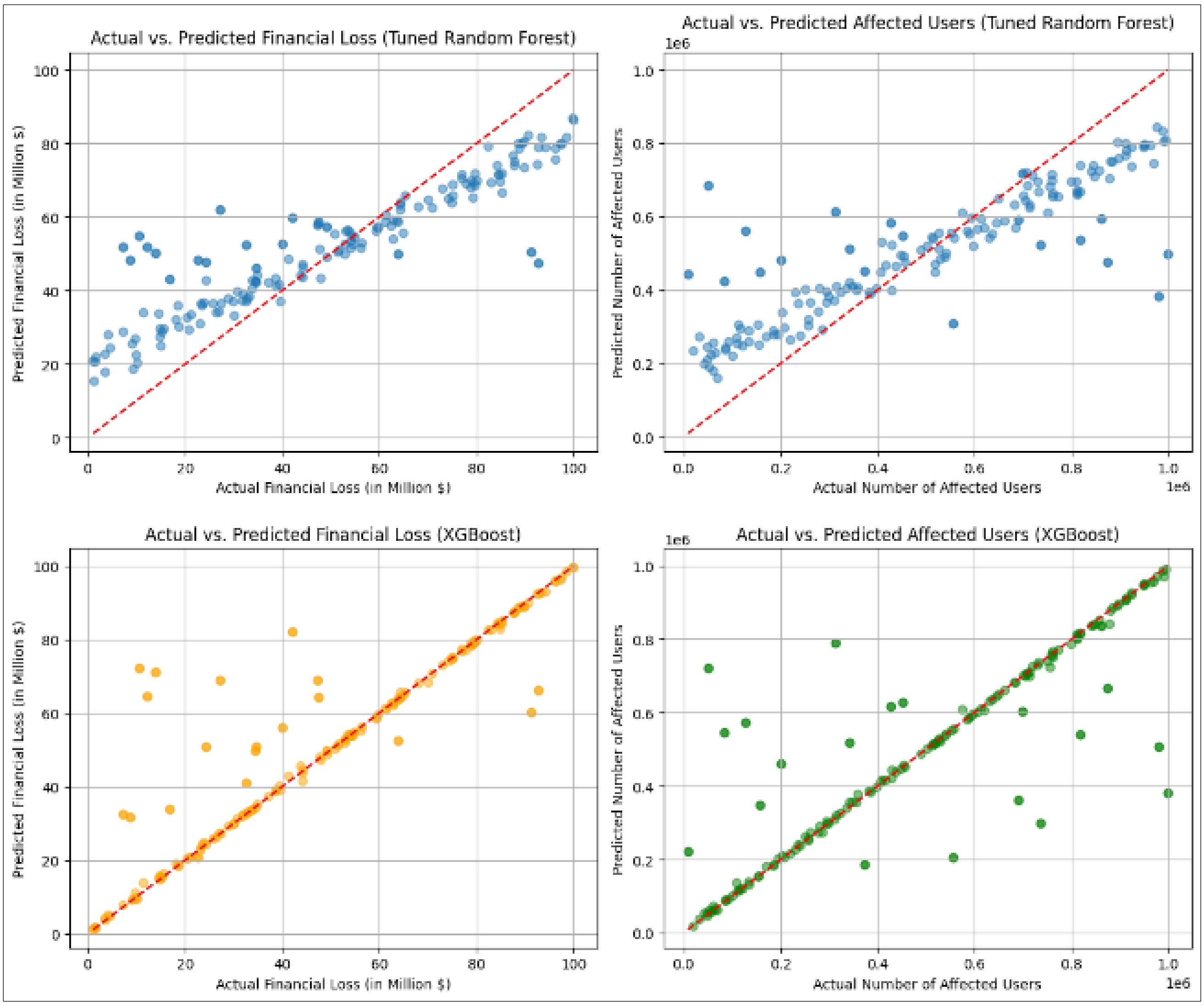

Figure 7 Model Performance Comparison: Actual vs. Predicted Financial Loss and User Exposure Using Tuned Random Forest and XGBoost

The scatter plots display the relationship between actual and predicted values for both financial loss and affected users, using Tuned Random Forest (top row) and XGBoost (bottom row) models. Both models show strong positive correlations, with points closely aligning along the red dashed line, indicating accurate predictions. XGBoost performs slightly better, with tighter clustering around the line for both financial loss and affected users, suggesting higher prediction accuracy compared to Tuned Random Forest, where some scatter is observed, particularly for Affected Users.

6. Discussion of Findings

The findings from this study highlight significant insights into the impact of cybersecurity incidents on financial losses and user exposure in the global financial sector. The analysis of total financial loss by attack source shows that nation-state actors and insider threats cause the highest financial damages, with losses amounting to $12,943.72 million and $12,839.28 million, respectively. These results emphasize the severity of cyberattacks originating from both politically motivated sources and internal actors who have direct access to sensitive financial data. The relatively lower losses from hacker groups and unknown sources suggest that the financial sector faces more considerable risks from targeted and internal attacks, highlighting the importance of enhanced monitoring and mitigation strategies for these specific threat vectors.

In terms of attack types, phishing emerges as the costliest cyberattack type, with a financial loss of $10,291.70 million, followed by DDoS attacks, man-in-the-middle attacks, and SQL injections. The dominance of phishing as a threat underscores its effectiveness in gaining unauthorized access to systems, often by exploiting human vulnerability through social engineering tactics. Additionally, DDoS attacks, while not directly breaching data security, cause significant disruption to services, leading to operational downtime and customer trust issues, which may contribute to long-term financial damage. This finding highlights the need for financial institutions to prioritize user education and implement advanced threat detection systems to address these common yet impactful attack methods.

The analysis of security vulnerabilities further reveals that social engineering and weak passwords are the most financially damaging, resulting in losses of $12,034.38 million and $11,781.00 million, respectively. These vulnerabilities highlight the critical need for better employee training and the adoption of multi-factor authentication systems to safeguard against unauthorized access. The role of unpatched software and zero-day vulnerabilities in causing financial losses also emphasizes the importance of timely updates and patch management systems within financial institutions to reduce exposure to advanced persistent threats (APTs).

Finally, the model performance results, particularly from the XGBoost model, show superior predictive accuracy compared to Linear Regression and Random Forest models for both financial loss and user exposure. With an R^2 of 0.74 for financial loss and 0.68 for user exposure, XGBoost outperforms the other models in capturing the complex, non-linear relationships between cybersecurity incidents and their outcomes. These findings suggest that XGBoost's ability to handle a large number of variables and complex interactions makes it a more effective tool for predicting the impact of cybersecurity incidents in the financial sector, offering valuable insights for institutions aiming to enhance their risk management strategies.

7. Conclusion

This study effectively demonstrated the application of Random Forest and XGBoost models in predicting financial losses and user exposure resulting from cybersecurity incidents in the global financial sector. XGBoost outperformed Random Forest, achieving higher accuracy (R^2 = 0.74) and lower error rates (RMSE = 14.52, MAE = 6.08) in predicting both outcomes, underscoring its capability to handle complex, non-linear relationships. Feature importance analysis highlighted Incident Resolution Time as the most critical factor in predicting financial loss, while Defense Mechanism Used and Attack Source were also important in the XGBoost model. Despite varying levels of effectiveness in defense strategies, phishing and social engineering were identified as the most financially damaging threats. These findings reinforce the value of machine learning in enhancing financial sector cybersecurity by offering precise predictions for better risk management. Further model optimization and class balancing techniques could improve detection accuracy, especially for minority threats.

Recommendations

Based on this conclusion, the study recommends that;

- Financial institutions should implement ongoing cybersecurity awareness training for employees to reduce vulnerabilities associated with human error, particularly in phishing and social engineering attacks. Educating employees about recognizing suspicious activities can mitigate risks, thereby reducing the likelihood of security breaches that lead to financial loss and user exposure.
- Institutions should invest in AI-driven threat detection systems capable of analyzing large volumes of data in real-time. These systems can identify unusual patterns in network traffic, potentially preventing breaches before they occur. Early detection would significantly reduce the impact of cyber incidents on both financial loss and user exposure.
- Organizations should develop and regularly update incident response protocols to ensure swift detection and mitigation of cybersecurity incidents. Timely responses minimize financial loss and reduce the duration of exposure to affected users. Having a well-coordinated, rapid-response system is critical to limiting the damage caused by cyberattacks.
- Financial institutions should enforce multi-factor authentication across all user accounts, especially for online banking and mobile applications. MFA reduces the likelihood of unauthorized access, particularly from phishing or credential-stuffing attacks, which are prevalent in the financial sector. This measure helps protect sensitive data, minimizing both financial loss and user exposure.
- Financial institutions should prioritize the regular updating of their IT infrastructure, including patching vulnerabilities in legacy systems. Unpatched systems are prime targets for cyberattacks like ransomware and data breaches. Ensuring that all systems are up-to-date significantly reduces the likelihood of breaches that could result in severe financial and reputational damage.

Compliance with ethical standards

Disclosure of conflict of interest

The authors confirm that there is no conflict of interest to be disclosed.

References

[1] Abdajabar, A., and Md Yunus, N. A. (2023). A Review on the Impact of Cybersecurity Crimes in Financial Institutions During the Time of Covid-19. Acta Informatica Malaysia, 7(1), 19-23.

[2] Aldasoro, I., Frost, J., Gambacorta, L., Leach, T., and Whyte, D. (2020). Cyber risk in the financial sector. SUERF Policy Note.

[3] Aldasoro, I., Gambacorta, L., Giudici, P., and Leach, T. (2023). Operational and Cyber Risks in the Financial Sector∗. International Journal of Central Banking, 341-402.

[4] Alkhdour, T., Shebab, R., Alwadi, B. M., Alrawad, M., Alismail, A. S., and Almaiah, M. A. (2024). Assessment of Cybersecurity Risks and threats on Banking and Financial Services. Journal of Internet Services and Information Security, 14(3), 167-190.

[5] Alsakini, S. A., Alawawdeh, H. A., and Alsayyed, S. (2024). The Impact of Cybersecurity on the Quality of Financial. Applied Mathematics and Information Sciences, 18(1), 169-181.

[6] Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper, 143, 1-29.

[7] Calliess, C., and Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. German Law Journal, 21(6), 1149-1179. doi:10.1017/glj.2020.67

[8] CERT Insider Threat Center. (2021). Insider Threat Study: Banking and Finance Sector. Software Engineering Institute, Carnegie Mellon University. (.

[9] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., and Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Geneva Papa Risk Insurance Issues Practice, 47(3), 698-736. doi: https://doi.org/10.1057/s41288-022-00266-6

[10] Erkan-Barlow, A., Ngo, T., and Goel, R. (2023). An in-depth analysis of the impact of cyberattacks on an in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States profitability of commercial banks in the United States. Journal of Global Business Insights, 8(2), 128-135.

[11] Ibrahimnur, A. A. (2023). Impact of Cybercrime on the Finance Sector: A Case of Banks in Nairobi County, Kenya (2008-2022). Journal of Public Administration, 1-90.

[12] Jimmy, F. (2024). Assessing the Effects of Cyber Attacks on Financial Markets. Journal of Artificial Intelligence General science, 6(1), 288-305. doi: http://dx.doi.org/10.60087/jaigs.v6i1.254

[13] Jin, J., Li, N., Liu, S., and Khalid Nainar, S. M. (2023). Cyber attacks, discretionary loan loss provisions, and banks' earnings management. Finance Research, 54, 103705.

[14] Jooda, T. O., Aghaunor, C. T., Kassie, J. D., and Oyirinnaya, P. (2023). Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. World Journal of Advanced Research and Reviews, 20(3), 2166-2177. doi:https://doi.org/10.30574/wjarr.2023.20.3.2424

[15] Lagarde, C. (2018). Estimating Cyber Risk for the Financial Sector.

[16] Luque, F. J., Lopez, J. M., and Williams, P. (2021). Cyber risk as a threat to financial stability. 181-211.

[17] Maheswari, U., Chaudhary, G., Manna, F., Khalane, V. P., and Muthukumar, E. (2024). Cybersecurity Challenges In Fintech: Assessing Threats And Mitigation Strategies For Financial Institutions. Educational Administration: Theory and Practice, 30(5), 1063-1071.

[18] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., and Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. World Journal of Advanced Research and Reviews, 21(3), 625-643.

[19] Pollmeier, S., Bangiovanni, I., and Slapnicar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. Journal of Safety Science, 159, 106022.

[20] Razavi, H., Jamali, M. R., Emsaki, M., Ahmadi, A., and Hajiaghei-Keshteli, M. (2023). Quantifying the Financial Impact of Cyber Security Attacks on Banks: A Big Data Analytics Approach. IEEE Canadian Conference on Electrical and Computer Engineering. doi:http://dx.doi.org/10.1109/CCECE58730.2023.10288963

[21] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., and Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. Journal of Healthcare, 8(2), 133. doi:https://doi.org/10.3390/healthcare8020133

[22] Shaddad, S. A. (2023). Effects of Cybercrime in E-banking Systems. 1-81.

[23] Shehab, R., Abrar, S., Almaiah, M., Alkhdour, T., Al Wadi, B. M., and Alrawad, M. (2024). Assessment of Cybersecurity Risks and Threats on Banking and Financial Services. Journal of Internet Services and Information Security, 14(3), 167-190. doi:http://doi.org/10.58346/JISIS.2024.I3.010

[24] Skinner, C. P. (2019). Bank Disclosures of Cyber Exposure. IOWA Law Review, 105, 239-281.

[25] Wang, V., Nnaji, H., and Jung, J. (2018). Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability. 1-39.