AGORA International Journal of Economical Sciences, http://univagora.ro/jour/index.php/aijes
ISSN 2067-3310, E-ISSN 2067-7669
Vol. 19, No. 2 (2025), pp. 460-472

A STATISTICAL STUDY FOR CYBERSECURITY RISK MANAGEMENT IN FINANCIAL INSTITUTIONS IN ALBANIA

D. VELIU, K. TIRANA, S. AHMETAJ

Denis Veliu[1], Kledia Tirana[2], Stelina Ahmetaj[3]
[1] Polytechnic University of Tirana, Tirana, Albania
https://orcid.org/0000-0002-6930-7292**,** Email: dveliu@fti.edu.al
[2]Universiteti Metropolitan Tirana, Albania
https://orcid.org/0009-0008-0772-4243, E-mail: ktirana@umt.edu.al
[3] Enti Kombetar I Operimit Rrugor, Albania
E-mail: stelinaahmetaj41@gmail.com

Abstract: *With the rapid development of technology and the digitalization of financial services, financial institutions are becoming increasingly vulnerable to cyber threats, which can seriously damage both the credibility and accessibility of customers and financial institutions. Cybersecurity has become a key issue in operational risk management for banks and financial institutions, requiring a robust regulatory and policy framework to protect sensitive data and financial assets. The purpose of this article is to examine cybersecurity risk management in financial institutions, with an emphasis on identifying common threats that are directly related to human and organizational contributions, such as ransomware, phishing, and social engineering. In this context, this study focuses on the role of human factors and the impact of employee awareness in preventing cyber incidents, highlighting the importance of continuous training and a strong organizational security culture. This study aims to assess the effectiveness of cybersecurity risk management practices in Albanian banks and financial institutions through literature review and survey methodology. This study contributes to a better understanding of the role of cybersecurity in financial risk management and suggests important steps to strengthen security measures and increase employee awareness.*

Keywords: *Cybersecurity, operational risk, social engineering, human factor, cyber awareness*

1 Introduction

In an increasingly digitalized and evolving world, financial institutions and not only, constantly face the risk of cyber attacks, becoming a target, due to the sensitive data and the large amount of transactions and monetary deposits they manage. Cyber Risk refers to the risk of financial loss, disruptions or reputational damage, which come from the failure of Information Security systems (Craigen, 2014, et al. p1). Often Financial Institutions are not able to provide an adequate set of tools, policies, trainings to protect networks, devices and programs from unauthorized access. This often leads to a decrease in customer confidence while using of digital financial services (DFS), thus creating a problem in financial inclusion and the development of financial markets (Dunn Cavelty, 2014).

The increase in cyber risks has prompted regulatory authorities and financial institutions to adopt stronger measures for risk management. International organizations such as the World Bank, the International Monetary Fund, and the Bank for International Settlements have proposed policies and guidelines to help banks and other financial institutions strengthen cyber policies in order to reduce the possibility of attacks.

The objective of this study is to analyze the ways of managing cyber risk in Financial Institutions, which include identifying, assessing and dealing with cyber attacks. Also the implementation of current policies and strategies in cyber risk management and their effectiveness.

The term "cybersecurity" refers to procedures, tools, and regulations intended to prevent unwanted access, damage, and attacks on networks, devices, software, and data. Cybersecurity has developed from a purely technical discipline to an essential part of corporate governance, economic stability, and national security in an increasingly digital environment (Von Solms & Van Niekerk, 2013). Cybersecurity has expanded to include security management, law, behavioral science, and strategic management as a result of the increasing frequency and destructiveness of cyber attacks.

According to the literature, cybersecurity is a problem as well as an operational and strategic challenge for businesses. The National Institute of Standards and Technology (NIST) states that good cybersecurity procedures guarantee the availability, confidentiality, and integrity of information systems referred to as "CIAs." Cybersecurity helps prevent unwanted access by those outside the business or institution and guarantees unfettered access to information by authorized users (NIST, 2024). Regardless of the technology and security measures employed, the truth is that no business is totally safe. Nonetheless, the world of cybersecurity is always changing, keeping up with new technology and implementing new regulations that call for improved risk and cyberattack management.

The severe repercussions of cybersecurity lapses in banks and other financial organizations are highlighted by recent market study (Uddin et al., 2020). These setbacks have prompted professionals in the field to look into the underlying reasons behind the increase in cyberattacks in the financial sector and develop practical mitigating techniques. Recent years have seen a rise in this field's literature and study. These consist of research investigations, policy documents, technical reports, and conceptual assessments. These resources provide a substantial contribution to our understanding of cybersecurity in general. The stability of the global financial system is threatened by cybersecurity risks, particularly in the absence of appropriate protection and risk management policies, according to recent academic research (Bouveret, 2019a; Bouveret, 2019b; Mugarura & Ssali, 2020; Humayun et al., 2020). Despite these developments, there is still a dearth of empirical study, mostly because it is hard to obtain reliable data. Despite the fact that the body of research on cybersecurity in the financial sector is expanding, there is a dearth of studies to expand on existing understanding and pinpoint areas that require more investigation. This gap emphasizes the necessity of conducting a thorough literature assessment that covers important topics affecting the financial industry in order to direct future research.

Overall, the existing literature shows that financial institutions face increasing financial distress as a result of frequent cyber incidents, an issue that has been exacerbated by the accelerated digitalization of financial services. Estimating the economic impact of cybersecurity breaches is inherently complex, as these incidents have multidimensional consequences on operational risk, cost structures, and institutional performance (Lewis & Baker, 2013; Peng et al., 2017; Lever & Kifayat, 2020). Ultimately, cybersecurity threats increase operational risk, which in turn increases costs and alters the financial outcomes of affected institutions (Kopp et al., 2017; Fitch, 2017; Aldasoro et al., 2020a; Aldasoro et al., 2020b).

It is widely recognized by industry experts, managers, and academic researchers that the increased likelihood of cybersecurity breaches significantly contributes to the increased operational risk for banks and financial institutions in a digital environment. Weaknesses in cyberinfrastructure, combined with social engineering techniques, create entry points for attackers seeking to access financial systems and disrupt operations (Willison & Warkentin, 2013; Longstaff et al., 2020; Smedinghoff, 2012; 2012; 2013; Gommans et al., 2015). The integration of cybertechnology has fundamentally changed the paradigm of operational risk management in the financial sector, especially in the context of a technology-based economy (Kröger, 2008; Biener et al., 2015). Traditional technological solutions, while necessary, are no longer sufficient, as no system is completely secure from hacking. This reality has transformed cybersecurity risk from an IT issue to a strategic board-level issue. (Aldasoro et al., 2020a) conducted one of the most comprehensive empirical studies to date, analyzing over 700,000 observations of operational losses related to cyber incidents from 2002 to 2019. The study found that the cost of risk ranges from 6 to 12 percent of an organization's total revenue, depending on the loss assessment method. Specifically, the study found that it took an average of 435 days after a cyber breach to fully realize the associated losses, highlighting the complexity and difficulty of detecting the losses associated with such incidents. Operational risk essentially arises from the potential for loss due to events that disrupt normal business processes. In a digital environment, institutions are increasingly vulnerable to system failures, software errors, and break-ins, many of which are the result of technological gaps and imperfections rather than individual negligence. These vulnerabilities are often exploited by cybercriminals to cause measurable direct losses (e.g. financial theft, data breaches, etc.) and significant indirect damages such as reputational damage, customer harm, and regulatory sanctions. In this context, cybersecurity threats enable the misuse of digital systems and data, increasing operational risks. Therefore, cyber risk management must go beyond technical defenses and include strategic oversight, cross-functional coordination, and continuous assessment of vulnerabilities and human factors (Soomro et al., 2016; Ralston et al., 2007; Dutta and McCrohan, 2002).

Our study hypotheses are as follows:

1. What are the primary cybersecurity threats that financial organizations now face?
2. How does the human element impact how financial institutions respond to cyberattacks?
3. How do cyber-attacks affect financial institutions' operations and finances?
4. How much can employee awareness and organizational culture help banks and financial services reduce cybersecurity risk?
5. What obstacles and constraints do financial institutions have when putting cybersecurity risk management techniques into practice?
6. If staff understanding is lacking, are technological measures enough to guarantee security?

2 Foundation and Research Method

2.1 Foundation

Cybersecurity has become a major operational issue in the financial sector due to the prevalence of cybercriminal activities, system failures, and fraudulent transactions that can harm banking operations (Aseef et al., 2005; Choo et al., 2007; Choo, 2011; Javaid, 2012; McCon 2013). Cybercriminals often use stolen personal identification numbers (PINs) of employees and customers to conduct fraudulent transactions (Veijalainen et al., 2006; Smedinghoff, 2012; Gommans et al., 2015). Such actions can result in direct financial losses and expose institutions to legal liability for privacy violations and fraud (Shackelford, 2012; Hon & Millard, 2018). In addition to identity theft, intentional disruptions such as DDoS attacks can completely disrupt banking services and create opportunities for attackers to penetrate systems with malware and spyware (Heeks, 2002; Gelenbe and Loukas, 2007; Beitollahi and Deconinck, 2007). In addition to compromising system availability, these attacks can damage hardware components and steal sensitive information. Although the causes of these disruptions are diverse, the operational impact of deliberate attacks is particularly severe and difficult to predict. Industry best practices for mitigating these risks include reconfiguring network infrastructure, patching hardware and software, and deploying DDoS mitigation solutions (Rubens, 2018).

However, cybersecurity threats continue to increase operational risks within financial institutions (Cebula & Young, 2010; Benaroch et al., 2012). Digital transformation has changed the nature of operational risk. Industry experts estimate that cyber risk currently accounts for 70-80% of total operational risk in the financial sector (Risk.net, 2016). Although the digitalization of the financial sector began several decades ago, the impact of digitalization on operational stability became particularly pronounced during and after the 2007-2008 global financial crisis. At that time, frequent changes in operating systems and lack of sufficient audit data made it difficult to attribute many failures in banking systems to specific technical reasons (Caruana, 2009; Francisco & Prevosto, 2010; Ames et al., 2015). Furthermore, the emergence of information technology-based financial engineering has led to the emergence of complex hybrid financial products whose risk profiles are difficult to assess without a robust cybersecurity infrastructure (Ralston et al., 2007; Cherdantseva et al., 2016). As a result, the global financial sector is now operating under a new operational risk regime, making financial institutions increasingly vulnerable to the impact of cyber incidents. This ever-evolving risk is blurring the lines between technical, technical, and human risks.

Cyber incidents can be caused by:

- Technological risks, like data loss, system failures, or communication breakdowns (Lewis, 2002; Patterson et al., 2002);
- Process risks, like transaction errors or settlement failures (Stoneburner et al., 2002; Embrechts et al., 2003; Power, 2005); and
- Human risks, like deliberate or inadvertent actions by staff, clients, or outside parties (Choo, 2011; Burden & Palmer, 2003; Holt & Lampke, 2010).

As a result, cybersecurity breaches can disrupt core banking functions and significantly increase operational risks, particularly in the areas of liquidity and credit risk. For example, a major cybersecurity incident can cause a short-term liquidity crisis, as customers may panic and withdraw funds quickly, reducing confidence in the bank's information security systems. Bouvret (2018) further points out that failures in payment and settlement systems increase the risk of bankruptcy. One such case is the First Investment Bank (FIB) depositor run in Bulgaria in 2014, which was triggered by rumors about the bank's liquidity. A study by Duffy and Younger (2019) of 12 U.S. financial institutions found that large-scale cyberattacks resulted in the immediate withdrawal of funds from large depositors, thereby threatening the institutions' solvency. To mitigate these impacts, banks may need to maintain higher liquidity reserves and invest in robust cybersecurity strategies to maintain market confidence. Additionally, cybercriminals are known to manipulate credit data such as loan information, defaults, and credit scores (Langton, 2018). Such manipulation increases the likelihood of inappropriate credit decisions being made and increases the credit risk of financial institutions. Cyber risks go far beyond IT outages. It now poses a systemic threat to financial stability due to its impact on liquidity, solvency, and solvency.

The field of cybersecurity is dynamic and constantly evolving, responding to new threats and optimizing technological solutions. Several upcoming trends and innovations are expected to shape the cybersecurity landscape, especially in the banking sector. A key advancement is the adoption of a zero trust model. This model operates on the principle of “never trust, always verify” and requires continuous approval from users and devices, regardless of location (Salim, Warsi, & Islam, 2023). As network complexity increases and remote working becomes more common, zero trust architectures provide greater protection against unauthorized access. Artificial intelligence (AI) and machine learning are playing an increasingly important role in cybersecurity. These technologies support threat identification, anomaly identification, and pattern recognition, enabling faster and more accurate responses to potential security incidents. The ability to process and analyze large data sets has become an essential tool in modern cybersecurity strategies. Advances in quantum computing pose major challenges to traditional cryptographic methods. To solve this problem, quantum-safe or quantum-proof cryptography is being developed to protect data from possible quantum attacks. Preparing for the post-quantum era is essential to maintaining the confidentiality and integrity of sensitive financial information. The deployment of 5G networks introduces new vulnerabilities due to faster speeds, an expanded network, and a larger attack surface. Securing 5G infrastructure is critical to protecting IoT devices, preventing exploitation of network vulnerabilities, and protecting critical systems. With the growing reliance on cloud services, the importance of cloud-based security solutions has increased. These solutions are specifically designed to protect cloud infrastructure, applications and data and address the unique challenges of cloud environments. The proliferation of Internet of Things (IoT) devices presents additional security risks and requires strict safeguards to prevent unauthorized access, data breaches, and tampering with connected devices. Securing the IoT ecosystem is becoming increasingly important for financial institutions. Homomorphic encryption, which allows calculations on encrypted data without decryption, offers a promising solution for maintaining data confidentiality and enables secure data processing. This technology has significant potential to improve cybersecurity in data-sensitive industries such as banking. Supply chain attacks targeting software and hardware vendors are a growing concern. Strengthening supply chain security is essential to prevent vulnerabilities that could compromise the integrity of products and services. The balance between data use and privacy is becoming increasingly important. Technologies that enable secure data analysis without exposing sensitive information are essential as data protection regulations evolve. Ransomware attacks are becoming increasingly sophisticated, highlighting the need for resilience strategies, including robust backup solutions and well-prepared incident response plans. Building organizational resilience is essential to minimizing the impact of ransomware incidents. Specifically in the banking industry, cybersecurity is rapidly evolving due to technological advances, increasingly sophisticated cyber threats, and the critical need to protect sensitive financial information. Integrating AI into cybersecurity has become a key strategy for improving threat detection, incident response, and risk management. Artificial intelligence technologies allow the analysis of large amounts of data, the identification of patterns and the adaptation to evolving threats, making them essential tools in modern bank defense systems.

AI-powered platforms, such as threat intelligence and anomaly detection systems, are used to strengthen defenses and proactively counter cyber threats. Implementing AI in cybersecurity not only involves technological advancements, but also requires collaboration between government agencies, financial institutions, and cybersecurity experts to ensure comprehensive protection across national and organizational boundaries. Case studies from the United States demonstrate the practical application of AI in addressing challenges such as insider threats, third-party risk management and cloud security. These examples highlight the importance of continuous monitoring, incident response preparedness and proactive risk mitigation strategies. However, adopting AI also comes with challenges, which highlights the need for responsible use. Finding a balance between innovation and ethical practice is essential to ensuring that AI technologies increase security without compromising fairness, privacy or transparency. Emerging technologies such as quantum secure cryptography, decentralized identity solutions and Zero Trust architectures represent the future frontiers of cybersecurity. As banks adopt these innovations, it becomes essential to develop adaptive cybersecurity strategies.

2.2 Research Method

This section's goal is to provide a thorough explanation of the research methodology, including study design, data collecting and processing, and statistical analyses utilized to determine the variables influencing financial sector workers' awareness of and behavior about cybersecurity concerns. Raising awareness of cybersecurity is crucial in a time when technology permeates every part of the financial system. Our study attempts to paint a clear picture of how workers respond to threats including phishing, social engineering, and illegal access.

The study is based on a quantitative approach, with a descriptive and correlational design. It uses a cross-sectional model, where data were collected at a single point in time (May 2025), through a structured electronic questionnaire.

The main population for this study includes employees in the Albanian financial sector, namely in second-tier banks, microfinance institutions, insurance companies and other institutions that manage sensitive digital information.

The final sample consists of 123 employees, selected through the non-probability convenience sampling method. This number represents a satisfactory distribution for statistical analysis with medium inferential power and allows for various tests with acceptable precision.

Table 1. *Sample composition*

Category	Number (N=123)	Percentage (%)
Commercial banks	72	58.5%
Microcredit institutions	31	25.2%
Insurance companies	20	16.3%

Table 2. *Position in the institution*

Position	Number (N=123)	Percentage (%)
IT Specialist /Risk	25	20.3%
Finance / Accountant	34	27.6%
Executive / Manager	21	17.1%
Operator / Front Desk	43	35.0%

Table 3. *Years of experience*

Years of experience	Number (N=123)	Percentage (%)
Less than 2 years	29	23.6%
2-5 years	38	30.9%
6-10 years	33	26.8%
More than 10 years	23	18.7%

A structured questionnaire, developed on the Google Forms platform and distributed via institutional email and professional communication groups, was used to collect data. The questionnaire contains 15 questions divided into 4 main sections:

1.Demographic and professional data
2.Knowledge and experience with cyberattacks
3.Behavior towards cyber risk
4.Evaluation of protection measures and training received

Most of the questions are on a 5-point Likert scale (1 = Not at all, 5 = Very much), some are closed-ended, and some are multiple-choice.

2.3 Statistical Analysis

After collection, the data were exported to Excel format and then transferred to SPSS v27 for statistical analysis.

Table 4. *Example of coding in SPSS*

Question	SPSS Code	Variable type	Value coding
Gender	gender	Nominal	1 = Male, 2 = Female
Position in the institution	position	Nominal	1 = IT, 2 = Finance, 3 = Manager, 4 = Front
Professional experience	experience	Ordinal	1 = <2, 2 = 2–5, 3 = 6–10, 4 = >10
Use of MFA	mfa_usage	Ordinal	1 = Never – 5 = Always
Cybersecurity training	training_received	Dichotomous	0 = No, 1 = Yes

Identifying phishing emails	phishing_identify	Ordinal	1 – 5
Willingness to report attacks	incident_report	Ordinal	1 – 5

For multiple-choice questions, each alternative was converted into a separate binary variable. Statistical analysis was divided into three levels:

1. Descriptive analysis

- Frequencies, percentages, mean and standard deviation were calculated for each significant variable.
- They were visualized through bar charts, pie charts and histograms to see the distribution of the data.

Table 5. *Descriptive data of participants (N = 123)*

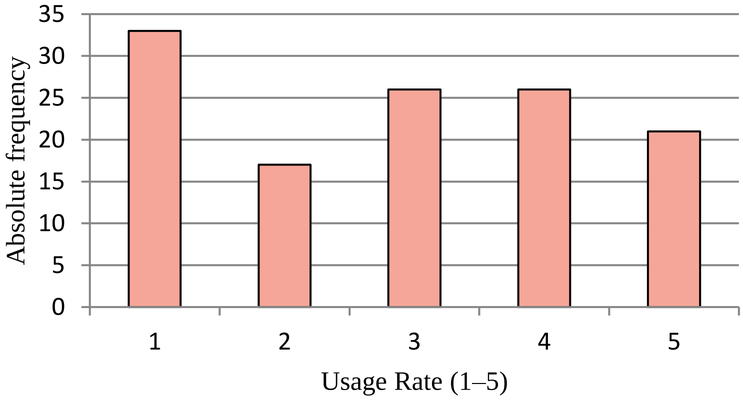
Variables	Value	Frequency (N)	Percentage (%)	Mean	Standard Deviation
Gender	Female	74	60.2%	-	-
	Male	49	39.8%	-	-
Using Two-Factor Authentication	YES	80	65%		
	NO	43	35%		
Training Participation	YES	86	70%		
	NO	37	30%		
Identifying Email Phishing (1–5)	-	-	-	3.8	0.9
Willingness to Report Incidents (1–5)	-	-	-	4.2	0.7

Descriptive analysis is a fundamental component of any empirical study, as it provides a summary of the main characteristics of the data collected. In this case, five key variables were analyzed to better understand the level of cybersecurity awareness and practices of the study participants.

The data collected in Table 5 shows that 60% of the participants are female, while 40% are male. This distribution indicates a dominance of female participation in this study. While this factor is not in itself a determinant of cybersecurity, it can serve as an indicator of the sensitivity or participation of different demographic groups in security topics.

The results show inthat 65% of participants stated that they use two-factor authentication (MFA). This is a positive indicator, as the use of MFA significantly increases the security of access to systems and personal information. However, the fact that 35% do not use this protection measure still shows room for improvement in user education. (figure 1)

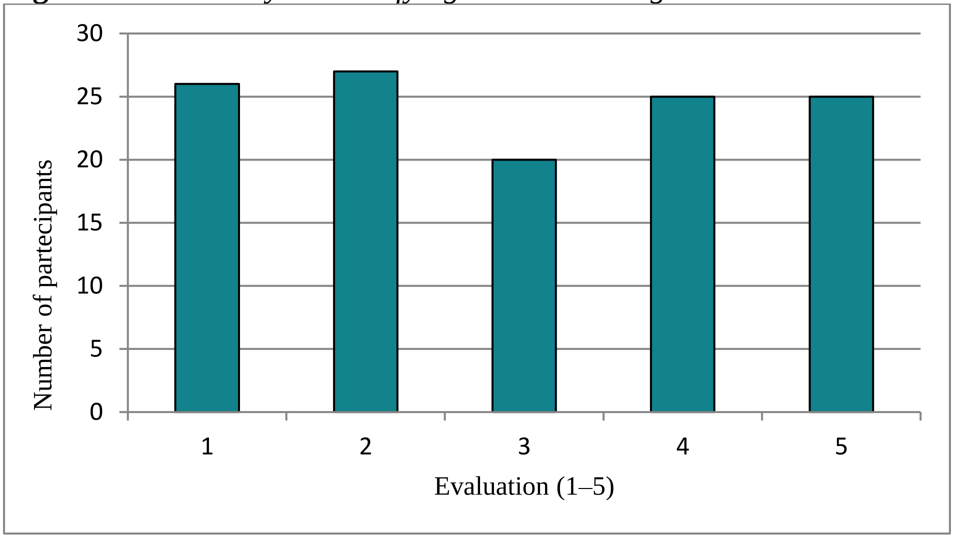
Figure 1. MFA Usage Histogram



Participation in training appears to be at a relatively good level, with 70% of respondents having participated in at least one training. This percentage is encouraging, as training is one of the most effective ways to build awareness and skills to prevent cyber risks. However, for the remaining 30%, additional educational intervention may be necessary.

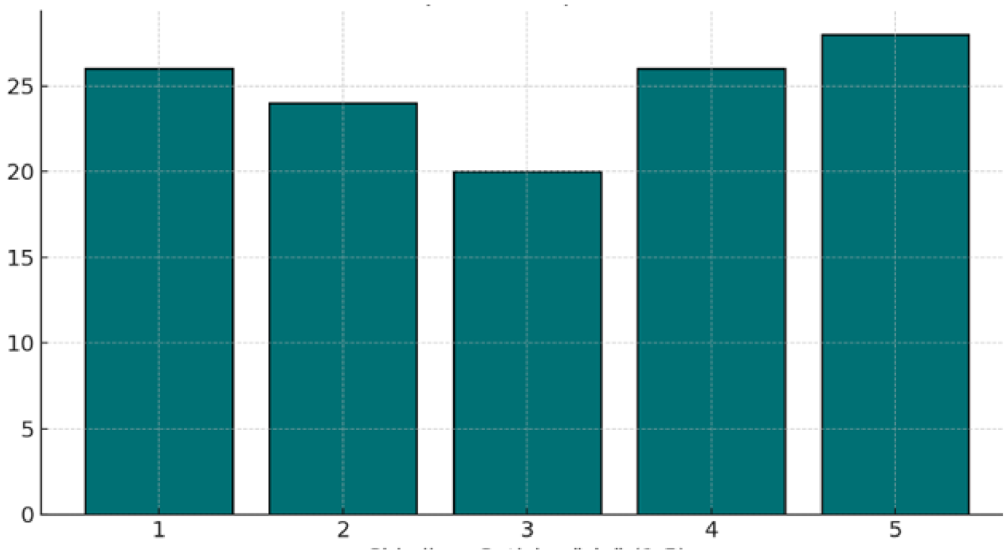
The ability to Identifying Email Phishing is measured as a variable on a Likert scale from 1 to 5, where 1 means "very difficult to identify" and 5 means "very easy to identify". The mean of 3.8 and standard deviation of 0.9 suggests that most participants feel relatively confident in their ability to identify fraudulent emails, but there is still a level of variation that implies the need for more practical education.(figure 2)

Figure 2. *The ability to Identifying Email Phishing*



In figure 3, participants were asked how willing they are to report cybersecurity incidents. The mean of 4.2 and the standard deviation of 0.7 indicate a very positive trend towards reporting. This is vital for the efficient management of incidents and the prevention of their spread. Overall, the descriptive analysis data shows a good level of security awareness and practices among participants. However, gaps still exist in areas such as universal use of MFA and inclusion in training, which need to be proactively addressed by institutions and organizations.

Figure 3. Willingness to report incidents



3 Results

3.1 Inferential analysis

The results from the inferential statistics aims to test different hypotheses of the study (Table 6), as follows:

•Hypothesis 1: There is a statistically significant relationship between professional experience and the use of security measures such as MFA.

Tested with: Chi-Square Test → Sig. = 0.003 → Significant relationship.

•Hypothesis 2: Employees who have received training are better able to recognize phishing emails.

Tested with: Mann-Whitney U Test → U = 1432.5, p < 0.001 → Significant difference.

•Hypothesis 3: Position in the institution affects the level of confidence to report attacks.

Tested with: Kruskal-Wallis H Test → H (3) = 12.78, p = 0.005 → Statistically significant effect.

Table 6. *Inferential analysis*

Hypothesis	Description	Statistical Test	Statistical value	P-value	conclusion
Hypothesis 1	There is a statistically significant relationship between professional experience and the use of security measures such as MFA.	Chi-Square Test	Sig. = 0.003	p = 0.003	Statistically significant relationship
Hypothesis 2	Employees who have received training are better able to recognize phishing emails.	Mann-Whitney U Test	U = 1432.5	p < 0.001	Important difference between groups
Hypothesis 3	Position in the institution influences the level of confidence to report attacks.	Kruskal-Wallis H Test	H(3) = 12.78	p = 0.005	Statistically significant effect by position

In this phase of the study, inferential tests were used to test important hypotheses related to cybersecurity in institutions. Each hypothesis was tested based on the nature of the data and the purpose of the analysis.

Hypothesis 1 aims to assess whether there is a relationship between the experience of professionals and the use of advanced security measures such as multi-factor authentication (MFA). Using the Chi-Square test, a p-value of 0.003 was obtained, indicating a statistically significant relationship between these two variables. This implies that experienced professionals are more likely to implement security measures such as MFA, which is a very important finding for human resource management and staff training planning.

Hypothesis 2 focuses on the effect of training on employees' ability to identify phishing emails. For this, the Mann-Whitney U test was used, as we are dealing with two independent groups (trained vs. untrained). The results showed a U value = 1432.5 and a p value < 0.001, suggesting that there is a statistically significant difference in the ability to identify cyber threats. This result highlights the importance of regular training to increase employees' awareness and competence towards cyber risks.

Hypothesis 3 analyzes whether the hierarchical position of the employee affects their confidence to report security incidents. Since we have more than two groups (e.g., technician, manager, middle manager, senior manager), the Kruskal-Wallis test was used. With an H value (3) = 12.78 and p = 0.005, the result shows a significant impact of position in the institution on self-confidence. This indicates that higher levels of management feel more confident to take action in cases of attacks, perhaps due to their involvement in decision-making processes and greater knowledge of security protocols.

In summary, all three hypotheses were found to be valid and support the idea that factors such as experience, training, and position in the institution play an important role in preparing for and responding to cyber threats. These findings can help organizations plan more targeted interventions and increase the effectiveness of their security systems.

3.2 Correlations

Spearman's Rho test was used, a nonparametric method to measure the strength and direction of the relationship between two ordinal variables or those that do not meet the assumptions for a Pearson correlation. This test is suitable for analyzing data that are not normally distributed, as well as for assessing relationships that may not necessarily be linear.

Spearman Rho was used to measure the relationship between:

- Training and confidence to report incidents → r = 0.43, p < 0.001
- Use of MFA and knowledge of social engineering techniques → r = 0.38, p = 0.002
-

Table 7. *Spearman correlations between key variables*

Variable pairs	**Spearman's Rho coefficient (r)**	**P-value**	**INTERPRETING**
Training and confidence to report incidents	0.43	< 0.001	Moderate and statistically significant positive correlation
Use of multi-factor authentication (MFA) and knowledge of social engineering	0.38	0.002	Moderate and statistically significant positive correlation

The Spearman Rho coefficient of 0.43 indicates a moderate positive association between training participation and employees’ confidence to report cybersecurity incidents. This suggests that the more trained employees are, the more confident they feel to take proactive steps in reporting attacks or attempted intrusions. The p-value < 0.001 makes this correlation statistically highly significant and not the result of chance.

The connection between the use of MFA and knowledge of social engineering techniques:

The Spearman coefficient of 0.38 suggests a moderate positive correlation between the use of multi-factor authentication (MFA) methods and employees’ general knowledge of social engineering techniques. The p value = 0.002 is also statistically significant, reinforcing the idea that individuals who better understand the risks of psychologically manipulated attacks are more likely to use advanced methods to protect their accounts, such as MFA.

These results show that educational interventions and active involvement in technical security measures not only affect individuals' practical preparation, but also their perception and self-confidence to be an active part of the institution's cyber defense system. This information is important for policymakers and institutional leaders who want to build a sustainable security culture in the workplace.

4 Conclusion

In conclusion, this paper on cyber risk management in financial institutions highlighted that digital transformation has brought numerous benefits, but at the same time has exposed the financial sector to greater cyber risks. The analysis clearly shows that cyber attacks, especially those that exploit the human factor through social engineering methods, represent a serious threat to financial institutions nationally and internationally. The main challenges identified are related to the lack of awareness and sufficient training of staff, the fragmentation of the regulatory framework and the still limited use of protection technologies such as multi-factor authentication and intrusion detection systems. However, best practices such as alignment with international standards such as ISO/IEC 27001, implementation of NIS2 guidelines and continuous training strategies point to a clear path to improving cyber resilience. Human security approaches recognize the human factor in cybersecurity and focus on education and the ability of people to make informed security decisions. Promoting a culture of cybersecurity awareness reduces the risk of human vulnerabilities. Evolving cybersecurity regulations and compliance standards reflect new technological developments and threats. To maintain strong cybersecurity and avoid legal consequences, it is essential to adapt to these regulatory changes. The growing demand for cybersecurity professionals highlights the need to expand cybersecurity education and training programs. Building a skilled workforce is essential to effectively confront emerging threats. Keeping pace with these trends and innovations is critical to ensuring resilience in the face of evolving cyber threats. Organizations must engage in continuous monitoring, proactive technology adoption, and fostering a strong cybersecurity culture as key components of a robust security strategy.

In conclusion, this article suggests that effective cybersecurity management in the financial sector requires the combination of three key components: technology, processes and human resources. Only through a global and integrated approach is it possible to achieve a satisfactory level of security that guarantees data protection and continuity of financial services.

REFERENCES

1. Ames, M., Schuermann, T., & Scott, H. S. (2015). Bank capital for operational risk: A tale of fragility and instability. *Journal of Risk Management in Financial Institutions*, *8*(3), 227-243.
2. Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach. (2020a). Operational and cyber risks in the financial sector. *BIS Working Paper No. 840*. Basel, Switzerland: Bank for International Settlements.
3. Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach. (2020b). The drivers of cyber risk. *BIS Working Paper No. 865*. Basel, Switzerland: Bank for International Settlements.
4. Aseef, N., Davis, P., Mittal, M., Sedky, K., & Tolba, A. (2005). Cyber-criminal activity and analysis. *White paper*.
5. Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems*, *13*(4), 357-381.
6. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131-158.
7. Beitollahi, H., & Deconinck, G. (2012). Analyzing well-known countermeasures against distributed denial of service attacks. *Computer Communications*, *35*(11), 1312-1332.
8. Bouveret, A. (2019a). Cyber risk for the financial services sector. *Journal of Financial Transformation (2019)*, *49*.
9. Bouveret, A. (2019b). Estimation of losses due to cyber risk for financial institutions. *Journal of Operational Risk*.
10. Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime—A new breed of criminal?. *Computer Law & Security Review*, *19*(3), 222-227.
11. Caruana, J. (2009), February. *Lessons of the financial crisis for future regulation of financial institutions and markets and for liquidity management*. Washington, DC: IMF.
12. Cebula, J.J., and L.R. Young. (2010). A taxonomy of operational cyber. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.
13. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.
14. Choo, K. K. R., Smith, R. G., McCusker, R., & Choo, K. K. R. (2007). *Future directions in technology-enabled crime: 2007-09*. Canberra: Australian Institute of Criminology.
15. Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & security*, *30*(8), 719-731.
16. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10).
17. Duffie, D., and J. Younger. 2019. Cyber runs. *Hutchins Center Working Paper #51*. Washington, DC: The Hutchins Center on Fiscal & Monetary Policy, Brookings Institution.

18. Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67-87.
19. Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, *20*(3), 701-715.
20. Embrechts, P., Furrer, H., & Kaufmann, R. (2003). Quantifying regulatory capital for operational risk. *Derivatives Use, Trading and Regulation*, *9*(3), 217-233.
21. Francis, L., & Prevosto, V. R. (2010). Data and disaster: the role of data in the financial crisis. In *Casualty Actuarial Society E-Forum, Spring 2010* (Vol. 62).
22. Fitch. 2017, April. Cybersecurity an increasing focus for financial institutions.
23. https://www.fitchratings.com/site/pr/1022468.
24. Gelenbe, E., & Loukas, G. (2007). A self-aware approach to denial of service defence. *Computer Networks*, *51*(5), 1299-1314.
25. Gommans, L., Vollbrecht, J., Gommans-de Bruijn, B., & de Laat, C. (2015). The service provider group framework: A framework for arranging trust and power to facilitate authorization of network services. *Future Generation Computer Systems*, *45*, 176-192.
26. Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. *The information society*, *18*(2), 101-112.
27. Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.
28. Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1–banks' use of cloud services. *Computer law & security review*, *34*(1), 4-24.
29. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189.
30. Javaid, A. (2013). Cyber security: Challenges ahead. *Available at SSRN 3281086*.
31. Kopp, E., L. Kaffenberger, and C. Wilson. (2017). Cyber risk, market failures, and financial stability, working paper. *International Monetary Fund* (WP/17/185).
32. Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, *93*(12), 1781-1787.
33. Langton, J. 2018, June 4. *Data breaches credit negative for BMO and CIBC: Moody's*. www.investmentexecutive.com: https://www.investmentexecutive.com/news/industry-news/data-breaches-credit-negative-for-bmo-and-cibc-moodys/.
34. Lever, K. E., & Kifayat, K. (2020). Identifying and mitigating security risks for secure and robust NGI networks. *Sustainable Cities and Society*, *59*, 102098.
35. Lewis, J. A., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage.
36. Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats* (p. 12). Washington, DC: Center for Strategic & International Studies.
37. Longstaff, T. A., Chittister, C., Pethia, R., & Haimes, Y. Y. (2000). Are we forgetting the risks of information technology?. *Computer*, *33*(12), 43-51.
38. McConnell, P., & Blacker, K. (2013). Systemic operational risk: does it exist and, if so, how do we regulate it?. *The Journal of Operational Risk*, *8*(1), 59.
39. Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10-28.
40. National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29
41. Patterson, D., Brown, A., Broadwell, P., Candea, G., Chen, M., Cutler, J., ... & Treuhaft, N. (2002). *Recovery-oriented computing (ROC): Motivation, definition, techniques, and case studies* (pp. 1-25). Technical Report UCB//CSD-02-1175, UC Berkeley Computer Science.

42. Peng, C., Xu, M., Xu, S., & Hu, T. (2017). Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, *44*(14), 2534-2563.
43. Power, M. (2005). The invention of operational risk. *Review of International Political Economy*, *12*(4), 577-599.
44. Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*, *46*(4), 583-594.
45. Risk.net. 2016, Jan 20. *Top 10 operational risks for 2016*. www.risk.net. https://www.risk.net/risk-management/2441306/top-10-operational-risks-for-2016#risk1.
46. Rubens, P. 2018, June 26. *How to prevent DDoS attacks: 6 tips to keep your website safe*. Nashville: eSecurity Planet, TechnologyAdvice. https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html.
47. Saleem, M., Warsi, M. R., & Islam, S. (2023). Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. *Journal of Information Security and Applications*, *72*, 103389.
48. Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, *55*(4), 349-356.
49. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International journal of information management*, *36*(2), 215-225.
50. Smedinghoff, T. J. (2012). Solving the legal challenges of trustworthy online identity. *Computer Law & Security Review*, *28*(5), 532-541.
51. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800-30.
52. Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management, 22(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2
53. Veijalainen, J., Terziyan, V., & Tirri, H. (2006). Transaction management for m-commerce at a mobile terminal. *Electronic Commerce Research and Applications*, *5*(3), 229-245.
54. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102
55. Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 1-20.