Cybersecurity Risk Awareness in Today's Financial Institution: The Case of Cameroon

Tani Schmidt Paul Ngo
Chief Technology Officer - Azire Cooperative Credit Union Limited
Lecturer at University Institute of Learning, Bamenda, Cameroon

***Abstract*— *The aim of this work is to raise awareness among the employees of a financial institution of the main Cybersecurity risks tha t affect financial institutions and how this can be mitigated and avoided to safeguard the institution from cyber threats: the case of Cameroon. Cybersecurity awareness refers to the knowledge and practices that employees of organizations possess to protect sensitive information and systems from computer threats. Today, Cybersecurity is the responsibility of every individual in an organization, from the top management position to the least. This is because of the growing rate of Cyberthreats on computer systems within financial institutions, as they have been witnessing a growing number of entities and individuals taking advantage of rapidly changing technological evolution, changes in human behavior, and technology failures to steal sensitive information or damage the reputation of an institution. This work outlines and explain s ten principal types of Cyberattacks that are common among financial institutions and further presents concrete procedures and guidelines that management can use to avoid and mitigate these attacks.*

***Keywords*— *Cybersecurity, Cyberthreats, Cyberattack.*

I. Introduction

The internet was born around the early 1960s; during this period, its design was limited to a few scientists, researchers, and the defense industry of the United States of America. During this era, computer crimes were limited to causing physical damage to the computer and related infrastructure. (Jeetendra Pande, 2017) According to Pande, around the 1980s, the trend changed from causing physical damage to computers to making a computer malfunction using a malicious code called a virus. Till then the effect was not so widespread because the internet was only confined to a few industries.

According to Buente and Robbin, when the internet was first made available to the general public in 1996, it quickly gained popularity as people gradually grew more reliant on it, to the point where it began to alter people's lifestyles in a variety of ways, including how they communicate, play, learn, and even work. (Buente & Robbin, 2008) The internet was so well-designed that users don't have to worry about how it works. Without worrying about where the data is stored, how it is transmitted over the internet, whether it can be accessed by another internet-connected person, or whether the data packet sent over the internet can be tampered with, users only need to click a few hyperlinks or type the desired information into a web browser from any location to obtain a result. (Jeetendra Pande, 2017)

As a result of this internet user’s behavior, the focus of the computer attacks shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. (Saleh, Rezk, & Barakat, July 2017) As more people use the internet, the frequency of these computer attacks keeps rising. For instance, in Cameroon, significant financial losses have been witnessed due to the activities of cybercriminals, with an average of 12.2 billion FCFA lost in 2021 alone, (Henri Kouam, 2024) Henri Kouam further narrates that the internet user base has been expanding geometrically, with over 12.73 million people in Cameroon who used the internet in 2024, accounting for about 43.9% of the country's total population. Also, Cameroon got the most financial institutions in the CEMAC Zone, counting 19 banks and more than 351 microfinances. (Henri Kouam, 2024) All this makes her a potential target for cybercriminals. Thus, the necessity to secure cyberspace to counteract these growing cyber threats. The aim of this study is to educate financial institution employees on the main Cybersecurity threats to which they may be exposed, as well as how to prevent and mitigate these threats to protect the organization from cybercrime, the case of Cameroon.

II. Related Works

Many researchers have examined the dangers of Cybersecurity risks faced by financial institutions and have proposed various solutions for controlling and preventing these risks. However, our study contributes to the existing research by emphasizing that, in today’s context, Cybersecurity is the responsibility of everyone within a financial institution, from top management to the lowest levels. Our study also distinguishes itself by identifying three significant causes of Cybersecurity risk: the rapid evolution of technology, changes in human behavior, and technology failures. Additionally, it offers concrete solutions for preventing and managing these risks.

Research works by Akinyele & Daniel, on building a culture of Cybersecurity awareness in the financial sector as a means to eradicate Cybersecurity risk, highlight the key elements involved in cultivating a Cybersecurity awareness culture within the financial institution. This work began by emphasizing the significance of Cybersecurity awareness, acknowledging the evolving threat landscape and the potential consequences of security breaches in the financial sector. (Akinyele & Daniel, 2024)

Another research from Pranav Sharma on Cybersecurity Risks in Digital Banking: A Financial Perspective, explores the evolving nature of Cybersecurity threats in digital banking, emphasizing the financial consequences of Cyberattacks on banks and their stakeholders. Pranav Sharma's research also highlights a big communication gap between financial institutions and their customers on Cybersecurity education. He further explains that the consequences of cyber incidents extend beyond immediate monetary losses, encompassing legal penalties, reputational damage, and loss of consumer trust. His findings underscore the urgent need for banks to invest in advanced security technologies, enforce stronger regulatory compliance, and actively engage in customer awareness initiatives as a means to curve the risk of Cybersecurity (Sharma, 2015)

Abdullah Mohammed Ibrahim researched on Cybersecurity threats in the financial sector, trends, and mitigation strategies presents a comprehensive examination of evolving Cybersecurity threats within the financial ecosystem, including phishing, ransomware, insider threats, and advanced persistent threats. Additionally, it examines modern mitigation approaches, placing a strong emphasis on adherence to regulations, Zero Trust Architecture, AI-based threat identification, and incident response frameworks. (Ibrahim, 2015).

III. Presentation of Common Cyberthreats in a Financial Institution

Today, a broad range of Cyberattacks exist, however in this section we will be discussing on common Cyberattacks that are commonly used against financial institutions. It is important to note that Cyberattacks could be internal or external to an organization. (Yuchong Li; Qinghui Liu, 2021) Yuchong & Qinghui further explained that an internal attack is an attack to the network or the computer system by persons with authorized access to the system. It is generally performed by dissatisfied or unhappy employees or contractors. The motive of the internal attacker could be revenge or greed. It is comparatively easy for an insider to perform a Cyberattack as he is well aware of the policies, processes, IT architecture and weakness of the security system. (Jeetendra Pande, 2017) While an external attack is an attack to the network or the computer system by persons with unauthorized access to the system. In an external attack, the attacker could either hired by an insider or an external entity or just individuals with personal motives to steal or disrupt services of an institution. (Yuchong Li; Qinghui Liu, 2021) Below are some common Cyberattacks commonly used against financial institutions:

a) Phishing as a Cyberattack That Affects a Financial Institution

According to Rajesh, Phishing is a kind of Cyberattack whereby the attacker impersonate a trusted entity to deceived an employee or a customer of a financial institution into revealing sensitive information like login credentials, account numbers, or some personal details. (Rajesh Tanti, 2024) Rajesh further narrates that Phishing generally involves the used of fraudulent emails, text messages, or fake websites that mimic the bank’s branding to deceive users into providing data or clicking malicious links. A Phishing attack is a kind of attack that exploits human trust to steal funds, sensitive information or gain unauthorized access into the system. There exist various forms of phishing attacks however the most common include email phishing, spear phishing, smishing, pharming, and whaling. The different kinds of Phishing attacks are dependent on the kind of communication method used to deceived the into revealing sensitive information or performing actions that compromise their security.

b) SQL Injection as a Cyber Attack That Affects a Financial Institution

An SQL injection attack in the financial industry is a type of cybersecurity threat whereby the attackers exploit vulnerabilities in a bank's web applications or database applications. This occurs when the attacker gains access to inject malicious SQL code into an input field, such as search bars, which enables them to manipulate the database and obtain unauthorized access to sensitive data. (Fairoz & Al., 2021)

c) Man in the Middle as a Cyberattack That Affects a Financial Institution

According to Danial Javaheri & Al., Man-in-the-Middle attacks are a type of cyber-attack in the financial industry whereby an attacker intercepts and potentially alters communication between a bank customer and the banking system, such as the bank's mobile application, without the knowledge of the bank or the account holder. In this kind of attack, the attacker gains access to the communication channel and thereby infect the user’s device with software that monitors traffic; they could also trick the user into visiting a fake bank website or a malicious server. (Danial Javaheri & Al., 2023) The exist different forms of man-in-the-middle attacks some common types include ARP spoofing, which redirects local network traffic; DNS spoofing, which sends users to fake websites by corrupting DNS records; Wi-Fi eavesdropping send a user to a malicious hotspot; SSL/TLS stripping, which forces a user to an unencrypted HTTP connection; and Man-in-the-Browser (MITB), where malware manipulates browser transactions

d) Cross Site Scripting (XSS) as a Cyberattack That Affects a Financial Institution

Cross-site scripting (XSS) is a cyber threat that can affect financial institutions that are handling sensitive financial data and are reliant on web applications or mobile applications for online banking. XSS occurs when an attacker injects harmful scripts into web pages, exploiting vulnerabilities in web applications to steal financial data or manipulate user interactions with the systems. (Danial Javaheri & Al., 2023)

e) Distributed Denial of Services Attacks (DDOS) as a Cyberattack That Affects a Financial Institution

A Distributed Denial-of-Service (DDoS) attack is a type cyberattack whereby an attacker overloads targeted servers or services with massive amounts of malicious internet traffic from multiple sources to make the targeted system unavailable to legitimate users. These attacks can cause significant disruption, leading to service outages, financial losses, and damage to an organization's reputation. (Yuchong Li; Qinghui Liu, 2021)

f) Ai Powered Attacks as a Cyberattack That Affects a Financial Institution

An AI-powered attack is a type of cyber security risks for financial institution that leverage artificial intelligence (AI) technologies to enhance their sophistication, speed, scale, and effectiveness. These attacks exploit AI's ability to analyze vast datasets, identify patterns, and adapt in real time, making them particularly dangerous for financial institutions, which hold sensitive customer data and large financial assets. (Fortinet, 2025)

g) Eves dropping Attacks as a Cyberattack That Affects a Financial Institution

According to Danial Javaheri et al., An eavesdropping attack is a type of cyberattack whereby a hacker secretly intercepts and accesses data as it travels between two communicating devices, often on an unsecured network. eavesdropping attack is also known as sniffing or snooping attacks, these attacks exploit weak or unencrypted network communications to steal sensitive information like login credentials or financial data without the users knowledge. (Danial Javaheri & Al., 2023)

h) Password Attacks as a Cyberattack That Affects a Financial Institution

According to Yuchong Li and Qinghui Lui, A password attack is a type of cyber-attack that can occur in a financial institution whereby the attackers attempt to gain unauthorized access to banking systems, accounts, or sensitive data by exploiting or cracking a user’s passwords. These attacks target user credentials, which are often the first line of defense for securing online banking accounts, employee access to banking systems, or customer financial data. (Yuchong Li; Qinghui Liu, 2021)

i) Drive–By Attacks as a Cyberattack That Affects a Financial Institution

A drive-by attack, also known as a drive-by download attack, is a type of cyberattack in a financial institution whereby a malicious script causes a program to download and install itself on a user device, without explicit permission or knowledge from the user. It can happen on any user device, running any operating system. Often, these attacks occur when the user navigates to and browses a compromised web page. (Sood & Zeadally, 2016)

j) Ransomware Attacks as a Cyberattack That Affects a Financial Institution

Ransomware is a type of cyberattack in a financial institution whereby the attacker prevents users from accessing financial files or systems by encrypting them and demands a ransom payment for their return. This kind of attack generally occurs through malicious email attachments, links, or compromised websites, leading to costly operational disruptions and data loss. Today’s ransomware attacks can involve double extortion, where attackers also steal data and threaten to leak it if a ransom payment is not made. (Danial Javaheri & Al., 2023)

IV. The Impact of Cyber Security Threats on Financial Institutions In Cameroon

According to Henri Kouam, the predominant financial institution in Cameroon is microfinance institution. The financial services given to low-income people or groups who are usually excluded from mainstream banking are referred to as microfinance. Most microfinance institutions focus on offering credit in the form of small working capital loans, sometimes called microloans or microcredit. (Henri Kouam, 2024) Henri Kouam further narrates how Microfinance plays a very important role in development of Cameroon, as they contribute to over 60% of Cameroon GDP and employs about 90% of Cameroonian workers according to the world food program, Cameroon counts a total of 351 microfinances as at 2023. While a report conducted by appecam counted 15 banks in Cameroon with over 2,809,986 account holders.

According to another report from the Cameroonian National Agency for Information and Communication Technologies (ANTIC), which is a Cameroonian government agency responsible for promoting and regulating the country's information and communication technologies sector, such as Cybersecurity, electronic certification, and internet regulation, Cameroon lost close to 12.2 billion FCFA to cybercrime in 2021. A detailed review of the 2021 figures shows financial losses amounting to 2.5 billion FCFA caused by intrusion into the public and private IT systems. Scams and phishing caused 6 billion FCFA losses, while skimming caused a 3.7 billion FCFA loss. Further, the country had lost close to 6 billion FCFA in 2019 from the activities of cybercriminals. (Orishas Finance, 2022)

Based on the above data and reports, it is clear that Cybersecurity is essential to protecting consumers' financial information if Cameroon's economy is to stay stable and satisfy consumer demands for cash. Therefore, it is crucial to educate employees of financial industry on the many Cybersecurity dangers and how to prevent and mitigate them in order to protect the sector from Cyber-attacks.

V. Control and Prevention of Cyberthreats in a Financial Institution

With today’s rapidly changing technological evolution, digital transformations of the financial industry have also been accelerated dramatically owing to the changing customer behavior, pandemic-led disruptions, and the increasing number of people working remotely. Financial institutions had to adapt to these changes, which made them lucrative targets for cybercriminals due to their vast financial assets and rich data resources, highlighting the urgent need to protect cyberspace. Effective Cybersecurity involves proactive prevention, detection, response, and recovery of any security breaches: Below are some key areas to consider:

a) Technical Controls

This has to ensure that the infrastructure of the financial institution meets the industrial cyber security standards this can be achieved in the following ways

- Implementation of multi-factor authentication for all internal logins, customer logins and access systems.

- Use encryption for all data to protect against unauthorized access to sensitive information.
- Adopt a policy of zero-trust, where no user or device is trusted by default all access must be verified and authenticated.
- Deploy firewalls, intrusion detection and prevention systems and also anti-malware systems to further boost the security of the infrastructure.
- Ensure all software's used in a financial institution are licensed and are regularly updated.
- Conduct continuous monitoring with the used of AI-driven tools for abnormalities.

b) Employee Training

Employees training is crucial in ensuring the cyber space is secured this is because intruders will only take advantage of a security weakness left by an employee, Employees training has to do with providing all employees of financial institution with adequate awareness and knowledge of the dangers of Cyberattacks an how it can be avoided or mitigate. Cybersecurity is not only the job of and IT department, all employees need to be aware that they can be misled to serve as a breach for Cyberattacks. Below are some points to consider when carrying out employee training:

- Provide regular Cybersecurity training to educate employees to recognize phishing attacks, proper data handling, and emerging threats like AI-generated scams.
- Run awareness campaigns to build a security conscious culture.
- Educate employees on how to monitor unusual behavior or activities without compromising user's privacy.

c) Risk Management and Compliance

It is the process of identifying, assessing, and mitigating potential threats to an organization's digital assets and information systems. It's a proactive approach to ensure business continuity to minimize the impact of cyberattacks. An effective way to control cyberattacks is to ensure the organization's information system complies with regulatory cybersecurity requirements. Here are some points to consider when building a risk management and compliance system.

- Develop and test an incident response plan, including breach notification protocols
- Establish vendor risk management programs to assess third-party security and include clauses for compliance in contracts.
- Perform regular risk assessments, security audits, and penetration testing to identify and prioritize vulnerabilities.
- Comply with local cybersecurity regulatory requirement agency like ANTIC in Cameroon

VI. Institutional and Operational Procedures

For cybersecurity to be effective within an institution the institution must put down certain policy and guideline for the usage of digital assets and data, this can be archived in the following ways:

- Foster a data-centric security model by classifying data by sensitivity and restricting access such that only authorized uses have access to the resources and data. This can be achieved by enforcing a strong identity and access management system.
- Invest in a robust backups and redundancy systems, to minimize downtime in case of any system failures.
- Collaborate with regulatory agency like ANTIC Cameroon for a newly discovered cyberthreats.
- Monitor for supply chain risks and diversify vendors and subcontractors to avoid single points of failure.

VII. Conclusion

The purpose of this study was to educate employees of the financial industry on the many cybersecurity threats that financial institutions face and how it can be prevented and mitigate in order to protect the industry from cyberattacks: the case of Cameroon. The finance industry is revolutionizing daily due to the rapidly advancing technological evolution and the increasing human demands as the industry is taking advantage of technology to improve on the products and services it offers to users. However, because of this, cybercriminals are taking advantage of this to steal resources, sensitive information and to damage the activities of the institution. In this work ten principal types of cyberattacks that are common among financial institutions were discussed. This includes phishing, SQL injection, man-in-the-middle, cross-site scripting, distributed denial of service, AI-powered attacks, eavesdropping, password attacks, drive-by attacks, and ransomware. We further discusses the impact of cyberattacks on financial institutions in Cameroon and concluded with concrete steps on how to control and prevent cyberattacks in a financial institution. Here four main topics were discussed, which include technical controls, employee training, risk management and compliance, and institutional and operational measures.

Cybersecurity in today's financial institutions is not just the IT department's job; it is the duty of all employees, from the highest level of management to the lowest. The need for cybersecurity and awareness is paramount because of the rise in cyberattacks caused by changing consumer behavior, rich data resources, and financial institutions' substantial financial assets. The primary cyberattacks that financial institutions frequently face were described in this study, after which the impact of these attacks on financial institutions was critically assessed. Finally, we discussed how employees can control and prevent cyberattacks.

References

[1]. Jeetendra Pande. (2017). Introduction to Cyber Security. Haldw ani: Uttarakhand Open University.

[2]. Akinyele, D., & Daniel, S. (2024). Building a Culture of Cybersecurity Awareness in the Financial Sector. International Journal of Applied Information Systems.

[3]. American_political_parties. (2013). In Routledge eBooks. In American political parties (pp. 132–134). https://doi.org/10.4324/9780203798492-39.

[4]. Buente, W., & Robbin, A. (2008). Trends in Internet information behavior, 2000-2004. Journal of the American Society for Information Science and Technology.

[5]. Danial Javaheri & Al. (2023). Cybersecurity Threats in FinTech: A Systematic Review. Expert Systems with Applications, 241(8):122697.

[6]. Fairoz & Al. (2021). SQL Injection Attacks Prevention System Technology: Review. Asian Journal of Research in Computer Science, DOI: 10.9734/AJRCOS/2021/v10i330242.

[7]. Fortinet. (2025). AI in Cybersecurity: Key Benefits, Defense Strategies, & Future Trends. Retrieved October 7, 2025, from Fortinet: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

[8]. Henri Kouam. (2024). Overview of the Microfinance Sector in Cameroon: Regulation and Prospects. Cameroon Economic Policy Institute(CEPI), 24(8).

[9]. Ibrahim, A. M. (2015). Cybersecurity Threats in the Financial Sector: Trends and Mitigation Strategies. ResearchGate.

[10]. Orishas Finance. (2022, March 10). News Financieres. Retrieved October 8, 2025, from ORISHAS FINANCE Digitalizing Africa: https://www.orishas-finance.com/actualite/fraudes-bancaires-le-cameroun-a-perdu-20-millions-en-2021-6158c38b?lang=en

[11]. Rajesh Tanti. (2024). Study of Phishing Attack and their Prevention Techniques. Interantional Journal Of Scientific Research In Engineering And Management, 08(10):1-8.

[12]. Saleh, H., Rezk, A., & Barakat, S. (July 2017). The Impact Of Cyber Crime On E-Commerce. ResearchGate.

[13]. Sharma, P. (2015). Cybersecurity Risks in Digital Banking: A Financial Perspective. International Scientific Journal of Engineering and Management.

[14]. Sood, A., & Zeadally, S. (2016). Drive-By Download Attacks: A Comparative Study. IT Professional, 18(5):18-25.

[15]. Yuchong Li; Qinghui Liu. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. ELSEVIER SCIENCEDIRECT, 8176-8186.