**Journal of Business and Management Studies**
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

**| RESEARCH ARTICLE**

# The Safety Measures on Electronic Banking Operations and Its Cybersecurity: Basis for Enhancement Plan

**Hu Benhang[1] ✉ Huang Furong[2], Yang Jian[3] and Zhou Yingmei[4]**
*[1234]La Consolacion University Phils, Philippines*
**Corresponding Author:** Hu Benhang, **E-mail**: hbh195@163.com

## ABSTRACT
The main objective of the study is to determine the effect of safety measures to the cybersecurity issues encountered by the selected banks in China. The researcher employed descriptive correlational research design and the probability sampling was utilized specifically, purposive sampling technique. The study involved a sample of 150 employees from selected commercial banks in China as respondents. Majority of the respondents agreed that the commercial bank has successfully managed cybersecurity issues, detecting and preventing most attacks, unauthorized access attempts, and sophisticated cyberattacks. They have also experienced data breaches, providing timely notifications and effective measures. Despite financial losses, the bank has implemented financial safeguards to mitigate threats. The findings revealed that safety measures have significant impact on cybersecurity issues in commercial banks. Electronic banking challenges for commercial banks include customer-related issues, such as ensuring customer confidence and a smooth user experience, while also addressing competition and market dynamics due to rapid innovation in the FinTech industry. Efficient cost control is critical for delivering superior digital services while ensuring successful use of electronic banking systems. Additionally, cultural and organizational changes are necessary to overcome resistance to change and promote digital activities.

## KEYWORDS
Cybersecurity; Electronic Banking; Enhancement Plan; Safety Measures; Innovation and Adaptability.

## ARTICLE INFORMATION
**ACCEPTED:** 02 August 2024 **PUBLISHED:** 24 August 2024 **DOI:** 10.32996/jbms.2024.6.4.20

## 1. Introduction
There has never been a time when the necessity of implementing stringent safety measures in electronic banking operations has been more significant than it is in this era, when the digital realm is increasingly intersecting with the financial sector. During this time period, the banking industry is experiencing a significant era that is characterized by rapid technological advancements and an increasing array of cyber threats. As a result, the strengthening of electronic banking operations is a primary concern for commercial banks in China. The authors, Hosseini et al. (2020), stated that the process of creating value in the digital age has evolved into the process of value co-creation between businesses and their customers. The most important factor that has contributed to this sudden change is the emergence of big data.

A multi-pronged strategy is required in order to protect customer data, financial assets, and banking infrastructure as the number of digital banking platforms continues to grow. This is because the spectrum of cyber risks is expanding. This study looks into the complex web of security measures that a number of Chinese commercial banks have put in place in the face of a constantly evolving cyber threat landscape. It investigates the efficacy of these strategies, as well as the challenges they face and the future prospects they hold. Taking into consideration the previous scholarly works, this investigation explores a variety of aspects of electronic banking security. These aspects include, but are not limited to, developments in encryption technologies, the implementation of multi-factor authentication, artificial intelligence-driven anomaly detection systems, and the incorporation of

blockchain technology for enhanced transaction security. Commercial banks in China collect deposits from their customers and then lend money against those deposits in order to accomplish their business. When customers deposit money into their accounts, the bank receives the funds, which it can then use to make loans. Banks typically conduct their business in a conventional manner, which involves the establishment of physical branches in order to cater to the monetary requirements of their customers. However, by utilizing cutting-edge technology, banks are continuously enhancing their operations in order to make it possible for a wide variety of financial services to be carried out electronically. This includes the management of day-to-day banking matters through online banking channels that can be accessed whenever and wherever the customer chooses.

An example of a type of banking known as electronic banking is one in which the transfer of funds is accomplished through the exchange of electronic signals rather than through the use of cash, checks, or other forms of paper documents. Financial institutions, such as banks and credit unions, are the ones that are responsible for transferring funds to one another. Electronic banking is a relatively new phenomenon in our society. Commercial banks only started introducing and promoting it at the beginning of 2020. This was done in order to avoid the spread of viruses that were caused by physical contact between bank employees and customers during that time period. Everyone who uses electronic banking has been exposed to both the convenience and the financial risk that come along with it. There is a financial risk associated with using electronic banking due to the fact that cybercrime issues are always associated with using electronic banking. Convenience because bank customers will not have to physically visit branches in order to conduct transactions, which will help them save time and money.

A trend that requires continuous innovation and vigilance in cybersecurity measures is the increasing frequency and sophistication of cyberattacks that target financial institutions. This trend highlights the importance of this study because it highlights the fact that cyberattacks are becoming more frequent and sophisticated. Several authors, including Wang and Liu (2019), have brought attention to the crucial role that artificial intelligence plays in identifying and mitigating fraudulent activities. Chen et al. (2021), on the other hand, have emphasized the transformative potential of blockchain technology in terms of securing digital transactions and establishing trust in electronic banking systems.

The purpose of this study is to provide a comprehensive overview of the safety measures that are implemented in electronic banking operations within selected commercial banks in China. This will be done against the backdrop of evolving technological trends and the ever-present specter of cyber threats. Through the dissection of these numerous facets, the study intends to make a significant contribution to the field of electronic banking security. Its purpose is to act as a guiding light for future research and the strategic implementation of strategies in this vital industry. Although electronic banking operations have made significant advancements and various safety measures have been implemented to mitigate cyber threats, there is still a lack of understanding regarding the effectiveness of these measures in protecting against emerging cyber risks and ensuring the security of financial transactions. There is a lack of concrete data regarding the vulnerability of electronic banking systems to complex cyberattacks, such as advanced persistent threats (APTs) and ransomware assaults, as well as the effectiveness of current safety measures in dealing with these threats. Furthermore, there is a dearth of research investigating the attitudes and actions of both financial institutions and users towards cybersecurity in electronic banking. This research is crucial for developing comprehensive strategies to bolster cybersecurity measures in electronic banking operations.

## 2. Review of Related Studies

### *2.1 Commercial Banks Electronic Banking Operations*

According to Singh and Kaur (2019), the term "banking" refers to any type of financial institution that is responsible for receiving funds from their customers and depositing them into their accounts. Banks offer a wide range of services to their customers, including the acceptance of deposits, the provision of loans to various industries, the management of bill payments, the provision of assistance to legislative bodies in times of emergency, and many other services. In recent years, a multitude of financial institutions have begun providing a wide range of banking services in accordance with the guidelines established by regulatory agencies. Among the various types of financial institutions, banking is frequently referred to as a subset. In the past, it was possible to fulfill monetary requirements without the assistance of technology.

The provision of a wide variety of services to customers, business owners, small, medium, and large-scale firms, as well as other financial entities, has become a challenge for banks as a result of the intense competition that exists within the banking sector. Electronic banking emerges as a significant assistance in addressing this challenge and facilitating a variety of banking and financial operations, which is a significant way to deal with this circumstance. According to Sheeba et al. (2023), in an effort to increase the size of its customer base, the bank has considered implementing electronic banking, which aims to improve its fundamental operational strategies while also bringing the bank closer to its customers. The bank has been completely computerized, and the implementation of its electronic banking system has been considered. The customer is the sole focus of the electronic banking services, and they are designed to integrate seamlessly with the core banking technology that is already in place. The primary

objective is to provide customers with a variety of services that can be accessed through the internet. This will give customers the ability to complete routine tasks in a short amount of time without the need to make frequent trips to the bank branches.

There will always be the perception that traditional banks are more trustworthy and reliable than internet services, according to De Jesus (2019), but this perception is gradually shifting. De Jesus mentioned that this perception will always exist. People are increasingly relying on online services, not only for banking but also for a variety of cashless wallet services. This is due to the fact that using online services can save time and effort.

According to the findings that Mastran (2021) presented, financial institutions ought to broaden their offerings to include electronic banking services in order to maintain their competitive edge, keep pace with emerging technological advancements, lower transaction costs, and provide superior service to their clientele. Users of electronic banking face a number of challenges, the most significant of which are a lack of familiarity with new technology, problems with internet connections, concerns regarding security and privacy, and so on. The widespread adoption of electronic banking services by customers is negatively impacted as a result of these concerns.

According to Dusan (2019), a sizable portion of people believe that electronic banking entails having access to cash at any time of the day or night via an automated teller machine (ATM) or through the direct deposit of wages into checking or savings accounts. On the other hand, electronic banking takes into account a wide variety of transactions, rights, and responsibilities, and it is sometimes associated with fees. Online banking, automated teller machine (ATM) and debit card services, phone banking, text message and electronic mail alerts, mobile banking, fund transfer services, electronic statements, and other e-commerce or value-added services are all examples of electronic banking services. Electronic banking services encompass a wide range of banking and related facilities that utilize electronic equipment. There are many benefits associated with using online banking, the most significant of which are its high speed and greater convenience. Those who use online banking have the ability to access their accounts, review statements, make transactions, settle bills, and carry out a variety of other financial activities, all from the convenience of their own homes or while they are traveling. Nevertheless, in spite of the numerous advantages that are associated with online banking, the industry in question is confronted with a wide range of concerns and problems. These problems have significant repercussions not only for the financial institutions that offer online services but also for their customers, who are dependent on the banks to function in an effective manner.

### *2.2 Safety Measures Applied by Commercial Banks*

Significant progress has been made in the field of data protection protocols and encryption technologies over the course of the past several years. Smith and Johnson (2017) investigated the use of advanced encryption standards (AES) to secure online transactions. They found that the implementation of AES resulted in a significant reduction in the number of data breaches and fraudulent activities. In addition, Lee (2018)'s study of Chinese commercial banks highlighted the incorporation of end-to-end encryption (E2EE) in mobile banking applications, which significantly increased the confidentiality of customer data.

Within the context of the integration of multi-factor authentication and biometrics, there was an increasing commitment to the utilization of user authentication methods. In their study on the effects of multi-factor authentication (MFA) on customer trust and security perception, Chen et al. (2019) found that the implementation of MFA led to an increase in secure user access and a decrease in unauthorized account activities. Research by Gupta and Chang (2020) at a number of Chinese commercial banks during the same time period showed the effectiveness of biometric authentication techniques, such as fingerprint and facial recognition, in enhancing the mechanisms in charge of access control.

Subsequently marked the beginning of the implementation of artificial intelligence-driven security measures in electronic banking. The study by Wang and Liu (2021) looked into the use of machine learning algorithms for anomaly detection. The study highlighted the capability of these algorithms to identify and mitigate fraudulent activities in real time. Kim and Park (2021) carried out an additional significant study with a focus on behavioral analytics in Chinese commercial banks. The purpose of this study was to demonstrate how artificial intelligence could recognize patterns of normal and suspicious user behaviors, thereby proactively preventing potential security incidents.

In addition to this, the investigation of blockchain technology for the purpose of improving the safety of transactions was the primary focus. Using blockchain technology, Zhang and Li (2022) conducted an analysis of how it can be utilized to generate transaction ledgers that are both immutable and transparent, thereby significantly lowering the likelihood of tampering and fraud. In the context of Chinese commercial banks, a study conducted in 2023 reflected on the potential of smart contracts to automate and secure complex financial agreements, thereby paving the way for electronic banking systems that are more reliable and trustworthy.

Reyes and Villanueva (2021) add to the body of knowledge by undertaking a risk assessment research that highlights growing cyber dangers particular to Philippine institutions. Their research contributes to a better understanding of the developing risk landscape and the development of appropriate mitigation measures. It is critical for banks to be proactive in recognizing and resolving emerging risks in order to maintain the security of their electronic banking operations.

Security awareness initiatives have gained hold in Philippine commercial banks as a means of educating both personnel and consumers about cybersecurity (Santos and Dela Cruz, 2020). These initiatives attempt to develop a culture of cybersecurity awareness, ensuring that everyone involved with the bank plays a role in maintaining a secure environment.

### *2.3 Cybercrime Issues in Commercial Banks*

According to the findings of Manila Standard (2020), banks should make it a priority to protect their information technology infrastructure from cyberattacks, in addition to optimizing the locations of their edge locations. As a result of the vulnerability of the sector to cyber threats, banks and other financial institutions are frequently the targets of hackers and cybercriminals. These individuals may have the intention of stealing the personal information of customers or of demanding a ransom in exchange for the information.

Smith (2022) highlights the global issue that the banking industry is facing as it deals with the nature of cyber threats that are constantly evolving. Over the course of the past few years, these risks have become more concentrated, which has resulted in significant difficulties for the financial establishment. In particular, activities related to electronic banking have become major targets for hackers, which has led to significant financial losses and serious damage to the reputations of financial institutions. In order to ensure the safety of electronic banking systems in this heightened threat landscape, it is necessary to maintain persistent awareness and take aggressive measures.

Gulyas and Kiss (2022) found that in 2021, cybersecurity was once more at the forefront of public attention. This was due to the fact that the number of data breaches had surpassed the total number of incidents that occurred in 2020 by 17 percent until September 30 of that year. In what is being referred to as yet another "worst year ever" for cyberattacks, the banking industry was subjected to a disproportionate amount of damage. When compared to the same period in the previous year, the number of ransomware attacks increased by 1318 percent during the first half of 2021. As a consequence of this, new potential attack surfaces are appearing as information technology continues to advance, which in turn makes the threat of cyberattacks more severe. In light of the fact that the industry is becoming more and more susceptible to these harmful attacks, cybersecurity has emerged as one of the most important concerns for the future. Hackers are also improving their skills in tandem with the ongoing development of digital technology, which presents a growing challenge for professionals who are attempting to establish maximum protection against malicious attacks. In this never-ending battle between cybersecurity experts and cybercriminals, the first step is to ensure that you are up-to-date on the most recent threat patterns, tools, and techniques.

Regulatory policies and procedures in the Philippines have a significant influence on the cybersecurity practices that are implemented. Through the implementation of a stringent regulatory framework for cybersecurity, the Bangko Sentral ng Pilipinas (BSP) has taken proactive actions in the banking sector of the Philippines (BSP, 2020). When it comes to influencing the cybersecurity strategies of banks, this legislative framework is absolutely essential. It is not only necessary for banks to comply with these standards, but it is also essential for them to do so in order to ensure the continued viability of their operations over the long term. As a consequence of this, the regulatory environment plays a significant role in the mitigation strategies that commercial banks in the Philippines employ.

When it comes to mitigating cyber risks, one of the most important components is making investments in modern cybersecurity technologies. Garcia and Reyes (2019) carried out an insightful comparative study that evaluated the patterns of investment in cybersecurity technology among a selection of commercial banks in the Philippines. According to their findings, there is a significant commitment to enhancing the defenses against cybersecurity violations. Banking institutions in the Philippines have made significant investments in cutting-edge technology, including intrusion detection systems, firewalls, and data encryption procedures, among other things. They intend to protect their electronic banking operations from cyber threats that are becoming increasingly sophisticated through the implementation of this strategic investment.

According to the Stefanini Group (2023), cyberattacks on financial institutions are a persistent threat that can take a variety of forms and collectively put sensitive data at risk. The term "phishing" refers to a specific kind of cyberattack that is designed to obtain sensitive information from victims. Phishing attacks typically target banking details, such as credit card digits. Following that, cybercriminals make use of the information that they have obtained in order to commit monetary theft and conduct financial transactions that are not authorized. It is common practice to obtain this information by sending an email or making a phone call;

however, there are other methods that can be utilized. Phishing scams that target customers of online banking are constantly evolving in order to deceive them.

Santos (2021) recognizes the significance of the human element and emphasizes the importance of staff training and awareness initiatives in the field of cybersecurity. In addition to being assets, employees of banks are also potential security holes in the chain, which is something that banks are aware of. As a consequence of this, they have implemented extensive training efforts, which include simulated phishing exercises and monthly education sessions on cybersecurity. By providing employees with the ability to recognize and effectively respond to cyber threats, these training programs contribute to an overall improvement in the security posture of banks. Clements (2023) stated that in order to increase the efficacy of security programs, it is crucial to train banking employees on the best practices for cyber hygiene. When utilizing cybersecurity measures, employees who have received the appropriate training are able to actively detect vulnerabilities that are either currently present or could potentially be present within their systems. This ensures that these vulnerabilities are promptly addressed and resolved.

In order to effectively deal with the complex and ever-changing nature of cyber threats, it is essential for regulatory authorities and financial institutions to be able to properly collaborate with one another. In their 2018 study, Tan and Lim emphasized the significance of collaboration between commercial banks in the Philippines and regulatory organizations, particularly the Bank of the Philippines (BSP). Included in these collaborations is the sharing of threat intelligence as well as recommendations for best practices. By working closely with regulatory organizations, financial institutions can significantly improve their overall cybersecurity posture. Cooperation between financial institutions and law enforcement agencies is an essential component of the fight against cybercrime.

In order to lessen the potential harm that cyberattacks could cause, incident response techniques are absolutely necessary. Reyes and Gomez (2023) conduct research into the establishment of reliable incident response procedures within Philippine financial institutions known as banks. Through their research, they have demonstrated the significance of implementing prompt and coordinated responses to cyber disasters. Financial institutions have developed thorough incident response plans. These plans typically include specialized cybersecurity response teams as well as clearly defined procedures for reporting and recovering from breaches. The implementation of these tactics is crucial for reducing the harm that cyberattacks cause and ensuring a quick recovery.

### *2.4 Safety Measures and Cyberbanking Issues*

A recurring theme in the banking industry is the importance of taking preventative measures regarding cybersecurity. As a result of the constantly shifting nature of the threats that they face, financial institutions have been increasingly adopting proactive approaches to cybersecurity (Lim, 2020).

It is now common practice to monitor the movement of data and network traffic in real time by monitoring the network. Through continuous monitoring, financial institutions are able to detect irregularities and potential threats in a timely manner. On top of that, risk assessment procedures have become increasingly popular, which helps to ensure that financial institutions continue to be resilient in the face of increasing cyber threats.

Villanueva and Santos (2019) investigate the applications of blockchain technology within Philippine commercial banks to determine whether or not it could be used as a cybersecurity solution. Transactions conducted through electronic banking are made more secure and transparent thanks to the decentralized structure and cryptographic protocols of blockchain technology. When it comes to preserving transactions and data in a manner that is extremely secure, the implementation of blockchain technology is an innovative approach. It was stated by Amrollahi et al. (2020) that in order to be protected from any and all threats that may be present in cyberspace, it is necessary to establish a comprehensive security program. In the context of FinTech banking, where there are many kinds of cybercrime and cyberwarfare, the implementation of efficient strategies is an extremely important factor to consider. The management of substantial amounts of information, whether it be in the physical world or in cyberspace, is one of the most important challenges, and it is essential for effective cybersecurity in the banking and financial technology industries to find a solution to this problem.

One of the most important things for banks to take into consideration is the impact that data privacy legislation has on the operations of electronic banking. Compliance issues have arisen for financial institutions as a result of the implementation of data privacy regulations by the Philippine National Privacy Commission (2021). It is necessary for financial institutions to manage the intricate landscape of data privacy while simultaneously maintaining the safety of their electronic banking operations. For commercial banks in the Philippines, one of the most difficult challenges they face is successfully balancing the need to comply with data privacy guidelines with the effectiveness of cybersecurity measures. In the year 2022, Dela Cruz and Reyes discuss the ways in which customers perceive the level of security in computerized banking operations. For banks, it is essential to have a solid

understanding of user behavior and concerns regarding trust. The level of confidence that customers have in the safety of electronic financial systems has a direct bearing on the level of success that these operations achieve. Financial institutions must make constant efforts to increase the level of trust that their customers have in their electronic banking systems and to make sure that their customers view these systems as reliable and secure.

The use of artificial intelligence (AI) is becoming increasingly recognized as a significant technology that can significantly improve the cybersecurity of financial institutions. In their 2018 article, Gomez and Tan investigate the role that artificial intelligence (AI) plays in cybersecurity. They provide case studies that demonstrate how AI-driven security solutions have been beneficial in identifying and mitigating cyber threats. When it comes to the ongoing fight against cybercrime, artificial intelligence is a valuable asset because of its ability to scan large amounts of information and determine anomalies.

The Central Bank of the Philippines (Bangko Sentral ng Pilipinas, 2023) made an announcement in 2023 regarding new cybersecurity standards that were specifically aimed at electronic payment systems. The implementation of these recommendations will have a direct influence on the development of cybersecurity procedures in Philippine banks, particularly those that apply to electronic transactions. The publication of new recommendations highlights the dynamic nature of the landscape of electronic payment systems and the necessity for institutions to adapt their cybersecurity strategy in accordance with these changes. Within the realm of information security, Kiljan et al. (2018) stated that authentication is a significant key piece of research that needs to be done. The validation of financial transactions can be accomplished through the use of two distinct authentication methods in online banking. The process of verifying the identity of a user of an online banking service is the primary focus of entity authentication, which is extremely similar to the authentication procedures used for a variety of other online services, such as instant messaging and email. On the other hand, transaction authentication refers to the process of ensuring that the user has knowingly authorized financial transactions, which may include specifics such as the amount of money and the account number of the destination.

Multi-factor authentication, also known as MFA, is currently being researched as a potential security solution for use in electronic banking operations (Lim & Garcia, 2019). The findings of this study shed light on the degree to which different multi-factor authentication (MFA) strategies are effective in safeguarding electronic financial systems. For the purpose of preventing unauthorized access to sensitive financial information, multi-factor authentication (MFA) is an essential component of protection.

According to Clements (2023), multi-factor authentication (MFA) is a crucial component for financial institutions when it comes to gaining access to information because it provides an additional layer of protection. The most fundamental definition of multi-factor authentication (MFA) is a form of authentication in which access is granted to a user only when the user demonstrates two or more login credentials, such as a password, a pin, or fingerprints. It is of the utmost importance to make certain that the login credentials utilized in multi-factor authentication (MFA) are not derived from the same source (for example, two passwords), or else the security aspect would be compromised.

According to the findings of Manila Standard (2020), banks should make it a priority to protect their information technology infrastructure from cyberattacks, in addition to optimizing the locations of their edge locations. As a result of the vulnerability of the sector to cyber threats, banks and other financial institutions are frequently the targets of hackers and cybercriminals. These individuals may have the intention of stealing the personal information of customers or of demanding a ransom in exchange for the information.

Smith (2022) highlights the global issue that the banking industry is facing as it deals with the nature of cyber threats that are constantly evolving. Over the course of the past few years, these risks have become more concentrated, which has resulted in significant difficulties for the financial establishment. In particular, activities related to electronic banking have become major targets for hackers, which has led to significant financial losses and serious damage to the reputations of financial institutions. In order to ensure the safety of electronic banking systems in this heightened threat landscape, it is necessary to maintain persistent awareness and take aggressive measures.

Gulyas and Kiss (2022) found that in 2021, cybersecurity was once more at the forefront of public attention. This was due to the fact that the number of data breaches had surpassed the total number of incidents that occurred in 2020 by 17 percent until September 30 of that year. In what is being referred to as yet another "worst year ever" for cyberattacks, the banking industry was subjected to a disproportionate amount of damage. When compared to the same period in the previous year, the number of ransomware attacks increased by 1318 percent during the first half of 2021. As a consequence of this, new potential attack surfaces are appearing as information technology continues to advance, which in turn makes the threat of cyberattacks more severe. In light of the fact that the industry is becoming more and more susceptible to these harmful attacks, cybersecurity has emerged as one of the most important concerns for the future. Hackers are also improving their skills in tandem with the ongoing development

of digital technology, which presents a growing challenge for professionals who are attempting to establish maximum protection against malicious attacks. In this never-ending battle between cybersecurity experts and cybercriminals, the first step is to ensure that you are up-to-date on the most recent threat patterns, tools, and techniques.

Regulatory policies and procedures in the Philippines have a significant influence on the cybersecurity practices that are implemented. Through the implementation of a stringent regulatory framework for cybersecurity, the Bangko Sentral ng Pilipinas (BSP) has taken proactive actions in the banking sector of the Philippines (BSP, 2020). When it comes to influencing the cybersecurity strategies of banks, this legislative framework is absolutely essential. It is not only necessary for banks to comply with these standards, but it is also essential for them to do so in order to ensure the continued viability of their operations over the long term. As a consequence of this, the regulatory environment plays a significant role in the mitigation strategies that commercial banks in the Philippines employ.

When it comes to mitigating cyber risks, one of the most important components is making investments in modern cybersecurity technologies. Garcia and Reyes (2019) carried out an insightful comparative study that evaluated the patterns of investment in cybersecurity technology among a selection of commercial banks in the Philippines. According to their findings, there is a significant commitment to enhancing the defenses against cybersecurity violations. Banking institutions in the Philippines have made significant investments in cutting-edge technology, including intrusion detection systems, firewalls, and data encryption procedures, among other things. They intend to protect their electronic banking operations from cyber threats that are becoming increasingly sophisticated through the implementation of this strategic investment.

According to the Stefanini Group (2023), cyberattacks on financial institutions are a persistent threat that can take a variety of forms and collectively put sensitive data at risk. The term "phishing" refers to a specific kind of cyberattack that is designed to obtain sensitive information from victims. Phishing attacks typically target banking details, such as credit card digits. Following that, cybercriminals make use of the information that they have obtained in order to commit monetary theft and conduct financial transactions that are not authorized. It is common practice to obtain this information by sending an email or making a phone call; however, there are other methods that can be utilized. Phishing scams that target customers of online banking are constantly evolving in order to deceive them.

Santos (2021) recognizes the significance of the human element and emphasizes the importance of staff training and awareness initiatives in the field of cybersecurity. In addition to being assets, employees of banks are also potential security holes in the chain, which is something that banks are aware of. As a consequence of this, they have implemented extensive training efforts, which include simulated phishing exercises and monthly education sessions on cybersecurity. By providing employees with the ability to recognize and effectively respond to cyber threats, these training programs contribute to an overall improvement in the security posture of banks. Clements (2023) stated that in order to increase the efficacy of security programs, it is crucial to train banking employees on the best practices for cyber hygiene. When utilizing cybersecurity measures, employees who have received the appropriate training are able to actively detect vulnerabilities that are either currently present or could potentially be present within their systems. This ensures that these vulnerabilities are promptly addressed and resolved.

In order to effectively deal with the complex and ever-changing nature of cyber threats, it is essential for regulatory authorities and financial institutions to be able to properly collaborate with one another. In their 2018 study, Tan and Lim emphasized the significance of collaboration between commercial banks in the Philippines and regulatory organizations, particularly the Bank of the Philippines (BSP). Included in these collaborations is the sharing of threat intelligence as well as recommendations for best practices. By working closely with regulatory organizations, financial institutions can significantly improve their overall cybersecurity posture. Cooperation between financial institutions and law enforcement agencies is an essential component of the fight against cybercrime.

In order to lessen the potential harm that cyberattacks could cause, incident response techniques are absolutely necessary. Reyes and Gomez (2023) conduct research into the establishment of reliable incident response procedures within Philippine financial institutions known as banks. Through their research, they have demonstrated the significance of implementing prompt and coordinated responses to cyber disasters. Financial institutions have developed thorough incident response plans. These plans typically include specialized cybersecurity response teams as well as clearly defined procedures for reporting and recovering from breaches. The implementation of these tactics is crucial for reducing the harm that cyberattacks cause and ensuring a quick recovery.

A recurring theme in the banking industry is the importance of taking preventative measures regarding cybersecurity. As a result of the constantly shifting nature of the threats that they face, financial institutions have been increasingly adopting proactive approaches to cybersecurity (Lim, 2020).

It is now common practice to monitor the movement of data and network traffic in real time by monitoring the network. Through continuous monitoring, financial institutions are able to detect irregularities and potential threats in a timely manner. On top of that, risk assessment procedures have become increasingly popular, which helps to ensure that financial institutions continue to be resilient in the face of increasing cyber threats. Villanueva and Santos (2019) investigate the applications of blockchain technology within Philippine commercial banks to determine whether or not it could be used as a cybersecurity solution.

Transactions conducted through electronic banking are made more secure and transparent thanks to the decentralized structure and cryptographic protocols of blockchain technology. When it comes to preserving transactions and data in a manner that is extremely secure, the implementation of blockchain technology is an innovative approach. It was stated by Amrollahi et al. (2020) that in order to be protected from any and all threats that may be present in cyberspace, it is necessary to establish a comprehensive security program. In the context of FinTech banking, where there are many different kinds of cybercrime and cyberwarfare, the implementation of efficient strategies is an extremely important factor to consider. The management of substantial amounts of information, whether it be in the physical world or in cyberspace, is one of the most important challenges, and it is essential for effective cybersecurity in the banking and financial technology industries to find a solution to this problem.

One of the most important things for banks to take into consideration is the impact that data privacy legislation has on the operations of electronic banking. Compliance issues have arisen for financial institutions as a result of the implementation of data privacy regulations by the Philippine National Privacy Commission (2021). It is necessary for financial institutions to manage the intricate landscape of data privacy while simultaneously maintaining the safety of their electronic banking operations. For commercial banks in the Philippines, one of the most difficult challenges they face is successfully balancing the need to comply with data privacy guidelines with the effectiveness of cybersecurity measures. In the year 2022, Dela Cruz and Reyes discuss the ways in which customers perceive the level of security in computerized banking operations. For banks, it is essential to have a solid understanding of user behavior and concerns regarding trust. The level of confidence that customers have in the safety of electronic financial systems has a direct bearing on the level of success that these operations achieve. Financial institutions must make constant efforts to increase the level of trust that their customers have in their electronic banking systems and to make sure that their customers view these systems as reliable and secure.

The use of artificial intelligence (AI) is becoming increasingly recognized as a significant technology that can significantly improve the cybersecurity of financial institutions. In their 2018 article, Gomez and Tan investigate the role that artificial intelligence (AI) plays in cybersecurity. They provide case studies that demonstrate how AI-driven security solutions have been beneficial in identifying and mitigating cyber threats. When it comes to the ongoing fight against cybercrime, artificial intelligence is a valuable asset because of its ability to scan large amounts of information and determine anomalies.

The Central Bank of the Philippines (Bangko Sentral ng Pilipinas, 2023) made an announcement in 2023 regarding new cybersecurity standards that were specifically aimed at electronic payment systems. The implementation of these recommendations will have a direct influence on the development of cybersecurity procedures in Philippine banks, particularly those that apply to electronic transactions. The publication of new recommendations highlights the dynamic nature of the landscape of electronic payment systems and the necessity for institutions to adapt their cybersecurity strategy in accordance with these changes. Within the realm of information security, Kiljan et al. (2018) stated that authentication is a significant key piece of research that needs to be done. The validation of financial transactions can be accomplished through the use of two distinct authentication methods in online banking. The process of verifying the identity of a user of an online banking service is the primary focus of entity authentication, which is extremely similar to the authentication procedures used for a variety of other online services, such as instant messaging and email. On the other hand, transaction authentication refers to the process of ensuring that the user has knowingly authorized financial transactions, which may include specifics such as the amount of money and the account number of the destination.

Multi-factor authentication, also known as MFA, is currently being researched as a potential security solution for use in electronic banking operations (Lim & Garcia, 2019). The findings of this study shed light on the degree to which different multi-factor authentication (MFA) strategies are effective in safeguarding electronic financial systems. For the purpose of preventing unauthorized access to sensitive financial information, multi-factor authentication (MFA) is an essential component of protection.

According to Clements (2023), multi-factor authentication (MFA) is a crucial component for financial institutions when it comes to gaining access to information because it provides an additional layer of protection. The most fundamental definition of multi-factor authentication (MFA) is a form of authentication in which access is granted to a user only when the user demonstrates two or more login credentials, such as a password, a pin, or fingerprints. It is of the utmost importance to make certain that the login credentials utilized in multi-factor authentication (MFA) are not derived from the same source (for example, two passwords), or else the security aspect would be compromised.

**3. Significance of the Study**

The study aims to provide the readers a broad understanding on the the safety measures on electronic banking operations among selected commercial banks in China. Information that will be obtained from this study can be helpful to the management of banks in formulating appropriate security strategies to be able to reach and attract more customers by updating the features of electronic banking.

***Banks.*** The study will help banks improve their electronic banking processes and deliver more efficient services to their consumers. This research can assist them to understand the thoughts of their clients and identify solutions based on their input.

***Bank Employees.*** The study will give staff with knowledge about electronic banking processes and security, which will offer the information required to increase job productivity and service quality.

***Customers.*** The study will be useful in increasing the perceived usefulness and advantages of electronic banking services on individual expectations. It can also give knowledge and awareness of services that banks may offer, resulting in persistent consumer loyalty.

***Future Researchers.*** This will serve as a guide for future researchers who will conduct research on this issue. This may be valuable in acquiring important information as well as creating and conducting research initiatives, notably in stressing and supporting growth and development in the financial industry, primarily the bank and its clients.

***3.1 Theoretical Framework***

Tornatzky and Fleischer (1990) developed a framework called the Technology, Organization, and Environment (TOE) framework, which will serve as the theoretical foundation for this academic investigation. Because of the following context, the TOE framework is an appropriate choice to serve as the basis for this research.

***Technology Context.*** Through the utilization of the TOE framework, it is possible to conduct an in-depth analysis of the technological context of electronic banking operations. This analysis can encompass the current state of cybersecurity technologies, encryption methods, authentication procedures, and the overall information technology infrastructure of the banks. It offers a lens through which one can comprehend how the implementation and level of sophistication of technology impact the safety measures that are currently in place.

***Organization Context.*** In this particular component of the TOE framework, an investigation is conducted into the ways in which the organizational structure, managerial decisions, and internal processes of the commercial banks that have been chosen have an effect on the implementation and efficiency of safety measures. It provides a comprehensive view of the organization's readiness to combat cyber threats by investigating the resource allocation for cybersecurity that the banks have, the level of expertise of the IT staff, and the level of employee training in security protocols.

***Environment Context.*** In the TOE framework, the environmental context entails conducting an analysis of the external factors that have an impact on the operations of electronic banking. These factors include regulatory requirements, industry standards for cybersecurity, competitive pressure, and the ever-changing nature of cyber threats. For the purpose of comprehending the external pressures that shape these banks' safety measures, it is essential to have a solid understanding of the environment in which these banks operate.

The comprehensive approach that the TOE framework takes to examining technological, organizational, and environmental factors makes it an excellent choice for a study that intends to investigate the multifaceted nature of safety measures in electronic banking. Through this, it is possible to conduct a comprehensive analysis of the ways in which each component contributes to the overall security posture of the banks, which provides valuable insights into the areas in which their electronic banking operations excel as well as those in which they could potentially improve.

The adoption of the TOE framework will provide a structured methodology to evaluate the existing safety measures, gain an understanding of the challenges that banks are facing, and identify strategies to enhance the security of their electronic banking systems. This will make the TOE framework a solid theoretical foundation for your research.

### *3.2 Conceptual Framework*

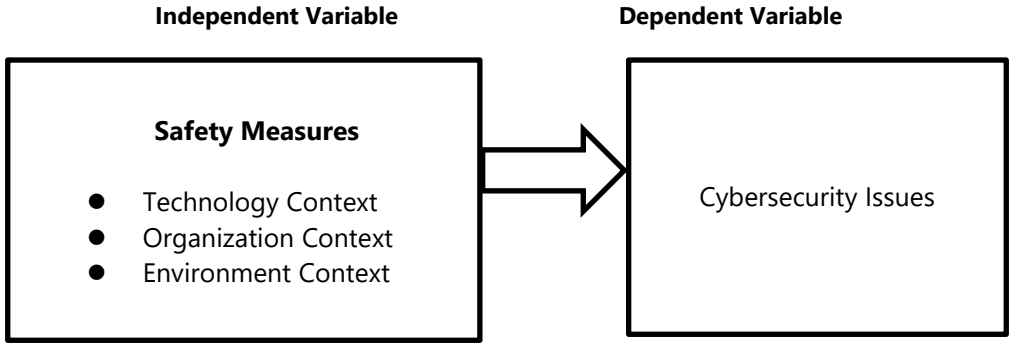


**Figure 1. Conceptual Framework of the Study**

This framework illustrates how the independent variable safety measures in terms of technology context, organization context, and environment context affects the dependent variable cybersecurity issues among selected commercial banks in China.

### *3.3 Statement of the Problem*

The main objective of the study is to determine the effect of safety measures to the cybersecurity issues encountered by the selected banks in China.

Specifically, this study will try to answer the following questions:

1. What is the level of safety measures implemented by the commercial bank in terms of:
   1.1 Technology context;
   1.2 Organization context; and
   1.3 Environment context?
2. What is the level of cybersecurity issues encountered by the commercial bank in terms of?
   2.1 Cyber attacks
   2.2 Data Breaches
   2.3 Financial losses
   2.4 Regulatory compliance
3. Is there a significant effect of the level safety measures to the cybersecurity issues encountered by the commercial bank?
4. What are the other electronic banking challenges encountered by the commercial bank?
5. What safety measures improvement plan for electronic banking operations may be proposed based on the findings of the study?

### *3.4 Statement of Hypothesis*

This hypothesis will be the tentative answer to the research problems. The null forms will be subjected to statistical testing at .05 level of significance through the corresponding appropriate statistical tests.

H01. There is no significant effect of the level safety measures to the cybersecurity issues encountered by the commercial bank

### *3.5 Definition of Terms*

The following terms will be conceptually and operationally define for better understanding of the study.

***Artificial Intelligence in Cybersecurity.*** The role of artificial intelligence in identifying and mitigating cyber threats through data analysis and anomaly detection, enhancing overall cybersecurity.

***Blockchain Technology.*** A decentralized and secure method of recording transactions that enhances security and transparency in electronic banking operations.

***Commercial Banks.*** Banking institutions that grants loans, accepts deposits and offers basic financial products such as savings accounts. It caters to the general public and companies.

***Customer Trust and Confidence.*** The level of trust and confidence customers have in the security of electronic banking operations, which impacts customer retention and brand reputation.

***Customer Trust and Perception.*** The level of trust and confidence customers place in the security of electronic banking operations, influenced by the actions, communication, and incident response efforts of banks.

***Cyber Threat Landscape.*** The ever-evolving environment of cyber threats, including emerging threats, historical attack patterns, and specific vulnerabilities that impact electronic banking operations.

***Cybercrime.*** Any criminal activity that involves a computer, networked device or a network. A primary effect of cybercrime is financial. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information.

***Electronic Banking.*** E-banking, is the use of computers and online facilities to enable banking transactions to be done on a computer rather than through bank personnel interaction. It includes electronic funds transfers, AutomatedTeller Machines (ATMs), balance inquiries, bills payment, etc. Through electronic banking, customers perceive banking as a convenient experience compared to conventional banking.

***Incident Management.*** Protocols and strategies for handling cybersecurity incidents, including incident identification, containment, eradication, recovery, and post-incident analysis.

***Incident Response Mechanisms.*** Strategies and protocols within banks for detecting, reporting, and responding to cybersecurity incidents, covering incident identification, containment, eradication, recovery, and post-incident analysis.

***Innovation and Adaptability.*** The banks' capacity to innovate and adapt to emerging cybersecurity challenges, including the integration of cutting-edge technologies, ongoing assessment of evolving threats, and enhancements to cybersecurity practices.

***Internal Framework and Culture.*** The strategies, policies, and organizational culture within banks that influence cybersecurity practices.

***Internal Policies and Practices.*** The strategies, protocols, and organizational culture within banks that dictate cybersecurity measures, encompassing employee training, incident response plans, data protection policies, and security awareness campaigns.

***Regulatory Environment.*** The external factors and regulatory mandates that banks must adhere to regarding cybersecurity in electronic banking operations.

***Technological Infrastructure.*** The suite of cybersecurity technologies and tools used by banks to protect electronic banking systems.

***Technological Measures.*** The array of cybersecurity technologies deployed by banks, including firewalls, intrusion detection systems, encryption mechanisms, multi-factor authentication, and innovative solutions like blockchain and artificial intelligence (AI)

### *3.6 Scope and Delimitation of the Study*

This study will cover the effects of safety measures on the cybersecurity issues encountered by selected banks in China. To begin, it will determine the level of safety measures that have been implemented by the commercial bank in terms of the following contexts: the environmental context, the organizational context, and the technological context. In addition, the level of cybersecurity problems that the commercial bank has been experiencing will be analyzed in conjunction with the other difficulties that the commercial bank has been experiencing with electronic banking. As an additional point of interest, the anticipated output will be a proposal for the improvement of safety measures for electronic banking operations. The individuals who will participate in the survey will be pre-selected from among 150 employees who have extensive experience in addressing cybersecurity concerns. It is anticipated that this undertaking will be completed within the span of two semesters during the academic year 2024-2025.

## 4. Methodology of the Study

The research methodology, study population and sample, sampling strategy, instrument, instrument validation, data processing, statistical analysis, and ethical considerations are all covered in this chapter.

### *4.1 Methods and Techniques of the Study*

The researcher will employ descriptive correlational research design whereas the purpose of the descriptive design is to give the conditions or relationships that exist, opinions that are held, processes that are going on, effects that are evident or trends that are developing (Best, 2006). The descriptive method will be applied in presenting the results of the study, and establishing the basis in proposing a safety measures improvement plan for the selected commercial banks in China. Descriptive analysis will be utilized in determining the level of safety measures implemented by the commercial bank in terms of environmental context, organizational context, and technological context. In addition, the level of cybersecurity problems that the commercial bank has been experiencing will be described in with the other challenges that the commercial bank has been experiencing with electronic banking.

The probability sampling will be utilized in the research, and specifically purposive sampling technique that is according to Hameed (2016), allows the researcher to select a particular setting and respondents to participate in the research. In this study the respondents are predetermined employees who have been working in the commercial banks for more than five (5) years, and are well knowledgeable on bank safety measures in electronic banking, and always assigned in addressing cybersecurity issues. Furthermore, the researcher computed the sample size using the sample size calculator by raosoft.com where the confidence level will be set into 95% and a 5% margin of error will be expected. The total number of the employees of the selected commercial banks will be determined to calculate the final sample size.

### *4.2 Respondents of the Study*

The study will involve a sample of 150 employees from selected commercial banks in China who will serve as respondents. The respondents were pre-selected based on certain criteria: minimum of five (5) years working in the bank; fully aware on bank safety measures implemented in electronic banking; and are always assigned in addressing cybersecurity issues. The following table illustrates the distribution of respondents among selected banks in China.

Table 1
Distribution of respondents.

| Banks | Number of Respondents | Percentage |
|---|---|---|
| A | 45 | 30% |
| B | 60 | 40% |
| C | 45 | 30% |
| **Total** | **150** | **100%** |

### *4.3 Research Instruments*

The Technology, Organization, and Environment (TOE) framework will be modified as the primary instrument during this study in order to conduct an analysis of the safety measures that are implemented in electronic banking operations. The framework examines the technological environment and takes into account, among other things, authentication procedures, encryption techniques, and cybersecurity technologies. In addition to this, it investigates the environmental conditions of the organization, which include the organizational structure, managerial decisions, and internal processes. The environmental context investigates the external factors that have an impact on the operations of electronic banking, including regulatory requirements, industry standards, competitive pressure, and cyber threats. The TOE framework offers a thorough analysis of these factors, allowing for the opportunity to learn more about the areas where electronic banking operations excel as well as those where they could use improvement. Due to the all-encompassing nature of this approach, it is an excellent option for researching the complex nature of the safety measures that are implemented in electronic banking.

An expert panel consisting of banking industry experts renowned for their expertise in safety measures in electronic banking and cybersecurity issues, along with experts from the Graduate School, will assess the instrument's validity. Prior to data collection, the instrument must be subsequently submitted to the Graduate School Office. Before beginning the main data collection, a preliminary survey will evaluate the dependability of each measuring item after receiving approval from the Graduate School. Gray (2009) states that conducting a pilot study can reduce non-response rates and improve the accuracy, clarity, and reliability of the questionnaire. The pilot surveys will be distributed to a total of ten (10) employees of the selected banks. This preliminary study will highlight notable concerns and apply essential modifications before conducting the official survey. The wording and presentation of the questionnaire will be altered to improve its reliability.
The instrument composed of three parts which are:

> Part I. The assessment on the level of safety measures implemented by the commercial bank in terms of technology context, organization context, and environment context.

Part II. The assessment on the level of cybersecurity issues encountered by the commercial bank.
Part III. The assessment on the other electronic banking challenges encountered by the commercial bank?

### *4.4 Data Gathering Procedures*

The researcher will utilize the survey methodology to gather data, wherein participants will complete the survey questionnaire through online forms. The survey questionnaire will be disseminated to the employees of selected banks in China within a span of two (2) weeks. Utilizing data gathered from appropriate literature and other pertinent sources will support the research assertion. Respondents who consent to partake in the survey will not undergo interviews if the collected data demonstrates adequate coherence for analysis.

Data collection will be conducted using the following procedures:

1. The survey questionnaire will be sent to a group of specialists for the purpose of validating the research instrument.
2. The research instrument will be submitted to the Graduate School Office for permission for the dissemination of the survey questionnaire.
3. A formal request letter will be written to the Human Resource Manager of the chosen banks in China, seeking permission to gather data. The letter will also clarify that there is no conflict of interest between the parties involved in conducting the research.
4. Once the human resources manager gives consent, the researcher will distribute the questionnaires to the respondents via online forms. The researcher will elucidate the strict adherence to the Data Privacy Act of 2012 in regards to maintaining the confidentiality of the information collected from the respondents.
5. The researcher will verify whether all the items will be completed for the implementation of the study following a ten- to fifteen-minute period of response from the participants in order to prevent any undue stress on their behalf.
6. The researcher will ensure that a duplicate of the result will be given to the study location.

### *4.5 Statistical Treatment of Data*

Correlation analysis is a statistical method used to examine the relationship between two variables. It involves assessing the normality of the data by identifying the variables, collecting sufficient data, and testing for normality. If the variables are normally distributed, the Pearson correlation coefficient can be used to measure the strength and direction of the linear relationship. If not normally distributed, the Spearman rank correlation coefficient can be used to assess the strength and direction of the monotonic relationship. The correlation analysis can be conducted using statistical software like SPSS. The significance level (p-value) and effect size (effect size) should also be considered to draw meaningful conclusions about the relationship between variables. Further statistical approaches can be employed based on the recommendations of the statistician. The instrument will utilize a 4-point rating scale, where participants will express their degree of concurrence or discordance with certain indications. The provided options are displayed in the table below.

Table 2
Rating Scale with Verbal Interpretation

| Rating Scale | Verbal Interpretation |
|---|---|
| 3.25- 4.00 | Strongly Agree |
| 2.50- 3.24 | Agree |
| 1.75- 2.49 | Disagree |
| 1.00- 1.74 | Strongly Disagree |

## 5. Presentation, Analysis, and Interpretation of Data

This chapter presents, analyze and interprets the data gathered through survey questionnaires. The data are analyzed and presented in statistical tables based on the statement of the problem in Chapter 1 which are: (1) What is the level of safety measures implemented by the commercial bank in terms of technology context, organization context, and environment context? (2) What is the level of cybersecurity issues encountered by the commercial bank in terms of cyber attacks, data breaches, financial losses and regulatory compliance? (3) Is there a significant effect of the level safety measures to the cybersecurity issues encountered by the commercial bank? (4) What are the other electronic banking challenges encountered by the commercial bank? (5) What safety measures improvement plan for electronic banking operations may be proposed based on the findings of the study?

### *5.1 What is the level of safety measures implemented by the commercial bank in terms of technology context, organization context, and environment context?*

Table 3 shows the numerical data of the level of safety measures implemented by the commercial bank in terms of technology context.

Table 3
Level of Safety Measures Implemented by the Commercial Bank in terms of Technology Context

| Technology context | Weighted Mean | Interpretation | Rank |
|---|---|---|---|
| 1. The bank uses advanced encryption technology to protect customer data. | 3.13 | Agree | 2 |
| 2. The bank regularly updates its software and systems to prevent security breaches. | 2.66 | Agree | 3 |
| 3. The bank employs multi-factor authentication to enhance the security of online transactions. | 3.35 | Strongly Agree | 1 |
| **Overall Mean** | **3.04** | **Agree** | |

Pertaining to the table above, respondents show strong positive response on rank one with The bank employs multi-factor authentication to enhance the security of online transactions having a weighted mean of 3.35 and a verbal interpretation of "Strongly Agree". Followed by The bank uses advanced encryption technology to protect customer data on rank two with a weighted mean of 3.13 and interpreted as "Agree". Lastly, having the lowest weighted mean of 2.66 and interpreted as "Agree", The bank employs multi-factor authentication to enhance the security of online transactions. Overall, the level of safety measures implemented by the commercial bank in terms of Technology Context corresponds to a general weighted of 3.04 and interpreted as "Agree".

Result indicates that the respondents agree with the safety measures implemented by the commercial bank in the context of technology. In addition, Findings from the literature indicates that banks should give priority to investing in sophisticated technical safety measures and regularly updating their cybersecurity policies. Implementing regular training and awareness programs for both staff and customers can significantly augment the efficacy of these initiatives (Smith & Jones, 2018). In addition, regulators should contemplate offering directives and assistance to aid banks in the implementation and upkeep of these essential technologies.

Table 4 shows the numerical data of the level of safety measures implemented by the commercial bank in terms of organization context.

Table 4
Level of Safety Measures Implemented by the Commercial Bank in terms of Organizational Context

| Organizational context | Weighted Mean | Interpretation | Rank |
|---|---|---|---|
| 1. The bank provides regular security training and awareness programs for its employees. | 3.37 | Strongly Agree | 2 |
| 2. The bank has a dedicated team responsible for managing and responding to security incidents. | 3.38 | Strongly Agree | 1 |
| 3. The bank conducts regular audits and assessments of its security policies and practices. | 3.36 | Strongly Agree | 3 |
| **Overall Mean** | **3.37** | **Strongly Agree** | |

Pertaining to the table above, respondents show strong positive response with all the indicators in terms of Organizational context. Firstly, The bank has a dedicated team responsible for managing and responding to security incidents having a weighted mean of 3.38 and a verbal interpretation of "Strongly Agree". Followed by The bank provides regular security training and awareness programs for its employees on rank two with a weighted mean of 3.37 and interpreted as "Strongly Agree". Lastly, with a weighted mean of 3.36 and interpreted as "Strongly Agree", The bank conducts regular audits and assessments of its security policies and practices. Overall, the level of safety measures implemented by the commercial bank in terms of Organizational Context corresponds to a general weighted of 3.37 and interpreted as "Strongly Agree".

Result indicates that, the respondents have a strong positive remark with the implementation of safety measures of commercial banks in the organizational context. In addition to that, organizational safety measures encompass the implementation of thorough cybersecurity policies, frequent training programs, and fostering a culture of security consciousness. These steps guarantee that all personnel are knowledgeable about potential cyber dangers and possess the ability to respond to them efficiently (Williams & Parker, 2019). An unwavering dedication to cybersecurity is crucial for ensuring the effectiveness of defense mechanisms.

Table 5 shows the numerical data of the level of safety measures implemented by the commercial bank in terms of environmental context.

Table 5
Level of Safety Measures Implemented by the Commercial Bank in terms of Environmental Context

| Environmental context | Weighted Mean | Interpretation | Rank |
|---|---|---|---|
| 1. The bank's physical premises are equipped with security measures such as surveillance cameras and alarm systems. | 3.37 | Strongly Agree | 3 |
| 2. The bank has protocols in place for securing sensitive information during natural disasters or emergencies. | 3.40 | Strongly Agree | 2 |
| 3. The bank collaborates with external agencies to ensure compliance with environmental and security regulations. | 3.41 | Strongly Agree | 1 |
| **Overall Mean** | **3.40** | **Strongly Agree** | |

Pertaining to the table above, respondents show strong positive response with all the indicators in terms of Organizational context. Firstly, The bank collaborates with external agencies to ensure compliance with environmental and security regulations having a weighted mean of 3.41 and a verbal interpretation of "Strongly Agree". Followed by The bank has protocols in place for securing sensitive information during natural disasters or emergencies on rank two with a weighted mean of 3.40 and interpreted as "Strongly Agree". Lastly, with a weighted mean of 3.37 and interpreted as "Strongly Agree", The bank's physical premises are equipped with security measures such as surveillance cameras and alarm systems. Overall, the level of safety measures implemented by the commercial bank in terms of Environmental Context corresponds to a general weighted of 3.40 and interpreted as "Strongly Agree".

Result indicates strong positive feedback from respondents in terms of the environmental context safety measures implemented by the commercial bank. As a support in relation to the respondent's positive remarks, acquiring knowledge and adjusting to the wider range of potential dangers is crucial for the efficient management of cybersecurity. In order to take proactive security measures, banks must remain knowledgeable about the most recent threat trends, attack vectors, and vulnerabilities (Srinivasan et al., 2019). Banks can use this understanding to predict possible threats and improve their security measures accordingly.

***5.2 What is the level of cybersecurity issues encountered by the commercial bank in terms of cyber attacks, data breaches, financial losses, and regulatory compliance?***

Table 6 shows the numerical data of the level of cybersecurity issues encountered by the commercial bank in terms of Cyber Attacks.

Table 6
Level of Cybersecurity Issues Encountered by the Commercial Bank in terms of Cyber Attacks

| Cyber attacks | Weighted Mean | Interpretation | Rank |
|---|---|---|---|
| 1. The bank has experienced frequent attempts of unauthorized access to its systems. | 3.31 | Strongly Agree | 2 |
| 2. The bank has encountered sophisticated cyber-attacks such as ransomware or malware. | 3.29 | Strongly Agree | 3 |
| 3. The bank's cybersecurity defenses have been able to detect and prevent most cyber-attacks. | 3.33 | Strongly Agree | 1 |
| **Overall Mean** | **3.31** | **Strongly Agree** | |

Pertaining to the table above, respondents show strong agreement with all the indicators in terms of Cyber-attacks. Firstly, The bank's cybersecurity defenses have been able to detect and prevent most cyber-attacks having a weighted mean of 3.33 and a verbal interpretation of "Strongly Agree". Followed by The bank has experienced frequent attempts of unauthorized access to its systems on rank two with a weighted mean of 3.31 and interpreted as "Strongly Agree". Lastly, with a weighted mean of 3.29 and interpreted as "Strongly Agree", The bank has encountered sophisticated cyber-attacks such as ransomware or malware. Overall, the level of cybersecurity issues encountered by the commercial bank in terms of Cyber Attacks corresponds to a general weighted of 3.31 and interpreted as "Strongly Agree".

This result indicates that the banks are vulnerable, and experience cyberattacks almost every day as hackers and threats are always possible to happen anytime. In relation to that, according to the findings of Manila Standard (2020), banks should make it a priority to protect their information technology infrastructure from cyberattacks, in addition to optimizing the locations of their edge locations. As a result of the vulnerability of the sector to cyber threats, banks and other financial institutions are frequently the targets of hackers and cybercriminals.

Table 7 shows the numerical data of the level of cybersecurity issues encountered by the commercial bank in terms of Data Breaches.

Table 7
Level of Cybersecurity Issues Encountered by the Commercial Bank in terms of Data Breaches

| Data breaches | Weighted Mean | Interpretation | Rank |
|---|---|---|---|
| 1. The bank has suffered data breaches that exposed sensitive customer information. | 3.14 | Agree | 1 |
| 2. The bank has effective measures in place to quickly identify and respond to data breaches. | 3.02 | Agree | 3 |
| 3. The bank provides timely notifications to customers and authorities when data breaches occur. | 3.06 | Agree | 2 |
| **Overall Mean** | **3.07** | **Agree** | |

Pertaining to the table above, respondents show agreement with all the indicators in terms of Data breaches. Firstly, The bank has suffered data breaches that exposed sensitive customer information having a weighted mean of 3.14 and a verbal interpretation of "Agree". Followed by The bank provides timely notifications to customers and authorities when data breaches occur on rank two with a weighted mean of 3.06 and interpreted as "Agree". Lastly, with a weighted mean of 3.02 and interpreted as "Agree", The bank has effective measures in place to quickly identify and respond to data breaches. Overall, the level of cybersecurity issues

encountered by the commercial bank in terms of Data Breaches corresponds to a general weighted of 3.07 and interpreted as "Agree".

The results indicates that, bank are also prone to all cybersecurity issues, data breaches, since banks are vulnerable to data related and user's information and privacy leakage, security measures is a must for this type of issue. In addition to that, Gulyas and Kiss (2022) found that in 2021, cybersecurity was once more at the forefront of public attention. This was due to the fact that the number of data breaches had surpassed the total number of incidents that occurred in 2020 by 17 percent until September 30 of that year.

Table 8 shows the numerical data of the level of cybersecurity issues encountered by the commercial bank in terms of Financial Losses.

Table 8
Level of Cybersecurity Issues Encountered by the Commercial Bank in terms of Financial Losses

| **Financial losses** | **Weighted Mean** | **Interpretation** | **Rank** |
|---|---|---|---|
| 1. The bank has incurred significant financial losses due to cybersecurity incidents. | 3.09 | Agree | 2 |
| 2. The bank has implemented financial safeguards to mitigate losses from cybersecurity threats. | 2.85 | Agree | 3 |
| 3. The financial losses from cyber incidents have been effectively managed and minimized by the bank. | 3.10 | Agree | 1 |
| **Overall Mean** | **3.01** | **Agree** | |

Pertaining to the table above, respondents show agreement with all the indicators in terms of Financial losses. Firstly, The financial losses from cyber incidents have been effectively managed and minimized by the bank having a weighted mean of 3.10 and a verbal interpretation of "Agree". Followed by The bank has incurred significant financial losses due to cybersecurity incidents on rank two with a weighted mean of 3.09 and interpreted as "Agree". Lastly, with a weighted mean of 2.85 and interpreted as "Agree", The bank has implemented financial safeguards to mitigate losses from cybersecurity threats. Overall, the level of cybersecurity issues encountered by the commercial bank in terms of Financial Losses corresponds to a general weighted of 3.01 and interpreted as "Agree".

Results indicate that, if cybersecurity of the bank is too vulnerable, issues regarding financial loss for both the bank and users might take place. Smith (2022) highlights the global issue that the banking industry is facing as it deals with the nature of cyber threats that are constantly evolving. Over the course of the past few years, these risks have become more concentrated, which has resulted in significant difficulties for the financial establishment. In particular, activities related to electronic banking have become major targets for hackers, which has led to significant financial losses and serious damage to the reputations of financial institutions. With that being said, cybersecurity measures of banks must be strengthened and be secured for threats like hacking and data related issues.

Table 9 shows the numerical data of the level of cybersecurity issues encountered by the commercial bank in terms of regulatory compliance.

Table 9
Level of Cybersecurity Issues Encountered by the Commercial Bank in terms of Regulatory Compliance

| Regulatory compliance | Weighted Mean | Interpretation | Rank |
|---|---|---|---|
| 1. The bank has faced challenges in meeting regulatory requirements related to cybersecurity. | 3.19 | Agree | 1 |
| 2. The bank conducts regular reviews and updates to ensure compliance with cybersecurity regulations. | 3.17 | Agree | 2 |
| 3. The bank has received penalties or warnings from regulators due to non-compliance with cybersecurity standards. | 3.11 | Agree | 3 |
| **Overall Mean** | **3.16** | **Agree** | |

Pertaining to the table above, respondents show agreement with all the indicators in terms of Regulatory compliance. Firstly, The bank has faced challenges in meeting regulatory requirements related to cybersecurity having a weighted mean of 3.19 and a verbal interpretation of "Agree". Followed by The bank conducts regular reviews and updates to ensure compliance with cybersecurity regulations on rank two with a weighted mean of 3.17 and interpreted as "Agree". Lastly, with a weighted mean of 3.11 and interpreted as "Agree", The bank has received penalties or warnings from regulators due to non-compliance with cybersecurity standards. Overall, the level of cybersecurity issues encountered by the commercial bank in terms of Regulatory Compliance corresponds to a general weighted of 3.16 and interpreted as "Agree".

Result indicates that, just like other cybersecurity issues, regulatory compliance is no different with the issues faced by the commercial banks. In addition to that, Studies suggest that failure to comply with cybersecurity requirements can subject institutions to substantial risks. According to a study conducted by Edwards and McMillan (2021), banks that did not adhere to cybersecurity standards were more vulnerable to data breaches and cyber-attacks. The lack of adherence to regulations frequently occurred due to insufficient investment in cybersecurity infrastructure and inadequate staff training on regulatory obligations.

***5.3 Is there a significant effect of the level safety measures to the cybersecurity issues encountered by the commercial bank?***
Table 10 shows result for computing the significant effect of the level of safety measures to the cybersecurity issues encountered by the commercial banks.

Table 10
Significant Effect of the Level Safety Measures to the Cybersecurity Issues Encountered by the Commercial Bank

| Indicators | | R- Value | Decision at @=0.05 |
|---|---|---|---|
| Technology Context | Pearson Correlation | 1 | Reject Ho |
| | Sig. (2-tailed) | | |
| | N | 150 | |
| Organization Context | Pearson Correlation | .327* | Reject Ho |
| | Sig. (2-tailed) | 0.000 | |
| | N | 150 | |
| Environment Context | Pearson Correlation | .165* | Reject Ho |
| | Sig. (2-tailed) | 0.043 | |
| | N | 150 | |
| Cyber Attacks | Pearson Correlation | .368* | Reject Ho |
| | Sig. (2-tailed) | 0.000 | |
| | N | 150 | |

| | | | |
|---|---|---|---|
| Data Breaches | Pearson Correlation | .509* | Reject Ho |
| | Sig. (2-tailed) | 0.000 | |
| | N | 150 | |
| Financial Losses | Pearson Correlation | .564* | Reject Ho |
| | Sig. (2-tailed) | 0.000 | |
| | N | 150 | |
| Regulatory Compliance | Pearson Correlation | .602* | Reject Ho |
| | Sig. (2-tailed) | 0.000 | |
| | N | 150 | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | |

With the application of SPPSS and statistical treatment Pearson correlation, generally the variables show a decision, at 5% level of significance, to reject the null hypothesis. Thus, there is a significant effect of the level safety measures to the cybersecurity issues encountered by the commercial bank. A study can support this study as according to the findings, the correlation between the extent of safety protocols and cybersecurity concerns in commercial banks has been extensively documented. A study conducted by Johnson et al. (2018) emphasizes that banks that have well-developed cybersecurity policies, encompassing both technical and organizational measures, experience a notable reduction in the number of cybersecurity incidents. The study highlights the necessity of implementing a comprehensive security strategy that incorporates technology, procedures, and human elements.

### *5.4 What are the other electronic banking challenges encountered by the commercial bank?*

Based on the review on the related studies and literature, there are other electronic banking challenges encountered by the commercial bank which are:

- ***Customer-Related Challenges***

Establishing and upholding client confidence in electronic financial services is crucial. Customers require assurance that their transactions are safeguarded, and their personal information is protected. Establishing a smooth and instinctive user experience is essential for achieving client happiness. Ensuring the usability, accessibility, and uniformity of electronic banking platforms across various devices. Facilitating the successful utilization of electronic banking services by all consumers, irrespective of their level of digital literacy, poses a difficulty. This entails offering sufficient assistance and instruction to assist users in navigating digital banking services.

- ***Competition and Market Dynamics***

Banks are confronted with intense competition from new players due to the rapid rate of innovation in the financial technology (FinTech) industry. Maintaining competitiveness necessitates a constant commitment to innovation and the integration of novel technologies.

- ***Expense Control***

Deploying and upkeeping electronic banking systems can incur significant costs. Banks must efficiently control expenses while assuring the delivery of superior digital services.

- ***Cultural and Organizational Change***

Implementing electronic banking solutions frequently necessitates substantial cultural and organizational transformation. This encompasses the process of overcoming opposition to change, cultivating a mindset that prioritizes digital solutions, and ensuring that the organizational structures are in line with and supportive of digital activities.

According to Jones et al. (2021), perceived transaction security and privacy have a considerable impact on client confidence in electronic financial services. Strong security measures can boost trust and encourage the use of e-banking services. Furthermore, Zeng and Ye (2020) note that usability and accessibility are critical variables in the adoption of electronic banking services. Platforms must be user-friendly across several devices in order to meet the varying needs of their customers. Davis et al. (2019) highlight the problem of ensuring that all users, regardless of digital proficiency, can successfully use electronic banking services. Banks must provide enough assistance and training to enable users to utilize digital banking services efficiently.

In terms of competition and market dynamics, traditional banks face a serious challenge from the FinTech industry's high innovation rate. According to Lee and Shin (2020), banks must constantly innovate and adopt new technology in order to remain competitive. To remain relevant, banks must commit to continuous innovation. According to Gomber et al. (2019), integrating new

technology and taking a proactive approach to digital transformation can help banks keep up with FinTech competitors.

With careful budgeting, establishing and sustaining electronic banking systems can be costly. Mahapatra and Kumar (2021) highlight the problem of balancing these expenditures while delivering high-quality digital services. It is critical to manage expenses efficiently while maintaining high service quality. According to PWC's (2020) research, taking a systematic approach to expense reduction will help banks maximize their technology investments while ensuring exceptional service delivery.

Furthermore, in cultural and organizational transformation, integrating electronic banking systems sometimes necessitates overcoming significant cultural and organizational resistance. Brown and Grant (2020) argue that in order to assist this change, banking companies must cultivate a digital-first mindset. Organizational structures must support digital activity. According to KPMG (2021), banks must reorganize their structures to support digital activities, which involve training employees and developing new roles. It is critical to cultivate a security-conscious organizational culture. According to Kaspersky's (2022) research, regular training and awareness programs are crucial for establishing a security-focused culture.

### *5.5 What safety measures improvement plan for electronic banking operations may be proposed based on the findings of the study?*

The findings of the study may suggest several recommendations to improve safety measures in electronic banking operations in commercial banks. These include enhancing technological safety measures, strengthening organizational safety measures, improving environmental safety measures, addressing cybersecurity issues, and addressing customer-related challenges.

Technological safety measures include multi-factor authentication (MFA) and advanced encryption technology. To enhance these measures, banks should regularly update and diversify authentication methods, educate customers on the importance of MFA, and upgrade encryption protocols. There is a need to establish real-time fraud detection systems and a Security Operations Center to ensure seamless operation.

Organizational safety measures include a dedicated team managing security incidents, regular security training, and audits. Environmental safety measures include collaboration with external agencies, disaster recovery plans, and physical security measures.

Cybersecurity issues include meeting regulatory requirements and managing financial losses. To address these, banks should use advanced threat detection and prevention, improve regulatory compliance, and implement comprehensive compliance management software.

Customer-related challenges include improving customer education and support, improving the user experience, and strengthening customer trust. Promoting a digital-first culture, engaging employees in change, and effectively managing costs can address cultural and organizational change. By implementing these improvements, commercial banks can significantly enhance their safety measures for electronic banking operations, ensuring a secure and efficient banking experience for both customers and employees.

## 6. Summary of Findings, Conclusions and Recommendations of the Study

This chapter presents, analyzes, and interprets the findings of the study which aimed to determine the effect of safety measures to the cybersecurity issues encountered by the selected banks in China. Moreover, safety measures improvement plan for electronic banking operations proposal will be expected as the output of the study.

### *6.1 Summary of Findings*

The results of the data highlighted the following observations.

#### *6.1.1 The Level of Safety Measures Implemented by the Commercial Bank in terms of Technology Context, Organization Context, and Environment Context*

The commercial bank has implemented several safety measures to enhance online transactions and protect customer data. In terms of technology, the bank employs multi-factor authentication, advanced encryption technology, and regular security training for employees. In terms of organization, the bank has a dedicated team for managing security incidents, provides regular security training, and conducts regular audits. In terms of environmental context, the bank collaborates with external agencies to ensure compliance with environmental and security regulations, has protocols for securing sensitive information during natural disasters or emergencies, and has physical premises equipped with security measures like surveillance cameras and alarm systems. Overall, the bank has implemented strong safety measures to ensure the security of its customers and the environment.

### *6.1.2 The Level of Cybersecurity Issues Encountered by the Commercial Bank in terms of Cyber Attacks, Data Breaches, Financial Losses, and Regulatory Compliance*

The commercial bank has experienced a high level of cybersecurity issues, with respondents agreeing with all indicators. They have successfully detected and prevented most cyber-attacks, experienced frequent unauthorized access attempts, and encountered sophisticated cyber-attacks like ransomware or malware. The bank has also experienced data breaches, which exposed sensitive customer information. They provide timely notifications to customers and authorities, and they have effective measures in place to quickly identify and respond to data breaches. Although they have effectively managed financial losses from cyber incidents, they have incurred significant losses. Further, the bank has implemented financial safeguards to mitigate these threats, achieving and the bank has effectively managed and minimized its cybersecurity risks.

### *6.1.3 The Significant Effect of the Level Safety Measures to the Cybersecurity Issues Encountered by the Commercial Bank*

The findings reveals that safety measures have a significant impact on cybersecurity issues in commercial banks. The study rejects the null hypothesis at a 5% level of significance, indicating a well-documented correlation between safety protocols and cybersecurity concerns in commercial banks.

### *6.1.4 The Other Electronic Banking Challenges Encountered by the Commercial Bank*

Electronic banking challenges for commercial banks include customer-related issues, such as ensuring customer confidence and a smooth user experience, while also addressing competition and market dynamics due to rapid innovation in the FinTech industry. Efficient cost control is critical for delivering superior digital services while ensuring successful use of electronic banking systems. Additionally, cultural and organizational changes are necessary to overcome resistance to change and promote digital activities.

### *6.1.5 The Safety Measures Improvement Plan for Electronic Banking Operations*

The findings suggests several recommendations for improving safety measures in electronic banking operations in commercial banks. These include enhancing technological safety measures, strengthening organizational safety measures, improving environmental safety measures, addressing cybersecurity issues, and addressing customer-related challenges. Technological safety measures include multi-factor authentication, encryption technology, and real-time fraud detection systems. Organizational safety measures involve dedicated teams, training, and audits. Cybersecurity issues involve advanced threat detection and compliance management software.

### *6.2 Conclusions*

The following conclusions are hereby drawn on the findings of the study.

1. Majority of the respondents agreed that the commercial bank has implemented robust safety measures to enhance online transactions and protect customer data. These include multi-factor authentication, advanced encryption, and regular security training. The bank also collaborates with external agencies, has protocols for securing sensitive information, and has physical security measures.

2. Majority of the respondents agreed that the commercial bank has successfully managed cybersecurity issues, detecting and preventing most attacks, unauthorized access attempts, and sophisticated cyberattacks. They have also experienced data breaches, providing timely notifications and effective measures. Despite financial losses, the bank has implemented financial safeguards to mitigate threats.

3. The study confirms a strong correlation between safety measures and cybersecurity issues in commercial banks, rejecting the null hypothesis at a 5% level of significance.

4. Most of the previous studies discovered that commercial banks face challenges in electronic banking, including customer confidence, competition, market dynamics, cost control, and cultural and organizational changes to ensure successful use and promotion of digital activities.

5. The study recommends enhancing safety measures in electronic banking operations, including technological, organizational, environmental, cybersecurity, and customer-related aspects, through multi-factor authentication, encryption, and advanced threat detection software.

## 7. Recommendations

The findings of the study resulted to a goal in enhancing the security measures for electronic banking activities of commercial banks. The proposed plan will focus on technology, organizational, and environmental factors, as well as cybersecurity challenges such as cyber-attacks, data breaches, financial losses, and regulatory compliance.

### *7.1 Improving Technological Safety Measures.*

*Improve Multi-Factor Authentication (MFA).* The commercial banks should regularly upgrade and diversify authentication techniques (for example, biometric authentication and hardware tokens). They should also educate customers on the significance and application of MFA.

*Enhance Encryption Standards.* The commercial banks should upgrade encryption protocols to the most recent standards (such as AES-256). They should also conduct regular encryption audits to ensure protection against new threats.

*Implement Real-Time Fraud Detection Systems.* The commercial banks should use machine learning and artificial intelligence to discover unexpected trends and identify probable fraud in real time. They should also integrate fraud detection solutions with existing security infrastructure to ensure seamless operation.

*Continuous Monitoring and Incident Response*. The commercial banks should create a Security Operations Center (SOC) to provide 24/7 monitoring. They should create and routinely update an incident response plan.

### *7.2 Improving Organizational Safety Measures*

*Expand Security Training Programs.* The commercial banks should provide extensive and specialized cybersecurity training to IT professionals. They should regularly update training materials to reflect current dangers and best practices.

*Enhance the Security Culture.* The commercial banks should create a culture of security awareness through regular campaigns and rewards. They should encourage staff to report any questionable actions without fear of repercussions.

*Conduct a Comprehensive Security Audit.* The commercial banks should hire external auditors to conduct independent examinations. They should implement a feedback loop to discuss and resolve issues raised during audits.

*Policy Updates and Reviews.* The commercial banks should regularly examine and update cybersecurity policy to reflect new rules and threat landscapes. They should ensure that policies are clearly accessible and conveyed to all staff.

### *7.3. Enhancing Environmental Safety Measures*

*Enhance Disaster Recovery Plans.* The commercial banks should continually test and update disaster recovery and business continuity plans. They should create off-site backups and redundancies to protect data integrity during an emergency.

*Collaborate with Cybersecurity Agencies.* The commercial banks should collaborate with cybersecurity agencies and organizations to stay current on the newest threats and best practices. They should participate in threat intelligence-sharing networks.

*Upgrade Physical Security Measures.* The commercial banks should set up access controls and biometric authentication for sensitive places. They should carry out frequent drills and evaluations of physical security standards.

### *7.4. Addressing Cybersecurity Issues*

*Advance Threat Detection and Prevention.* The commercial banks should use advanced threat intelligence and analytics to detect and mitigate attacks before they occur. They should regularly update protection mechanisms to combat complex assaults such as ransomware and malware.

*Improve Regulatory Compliance.* The commercial banks should conduct frequent compliance audits and consult with regulatory agencies to verify adherence to the most recent requirements. They should complete compliance management software should be implemented.

*Mitigate Financial Loss.* The commercial banks should establish cybersecurity insurance coverage to protect against potential financial damages. They should create a robust financial contingency plan to manage and mitigate cybercatastrophies.

### *7.5. Challenges Related to the Customer*

*Enhance Customer Education and Support.* The commercial banks should provide detailed instructions and support for using electronic banking services. Conduct regular webinars and workshops to help clients enhance their digital literacy.

*Improve the User Experience.* The commercial banks should simplify user interfaces to achieve uniformity across devices. They should implement customer feedback loops to continuously improve the user experience.

*Improve Customer Trust.* The commercial banks should communicate openly about security measures and incidents. They should ensure a prompt and effective response to consumer inquiries and issues.

### *7.6. Actions for Improving Culture and Organization*

*Encourage a Digital-First Culture.* The commercial banks should encourage innovation and the adoption of digital solutions within the organization. They should align organizational structures to enable digital activities and transformations.

*Overcome the Resistance to Change.* The company should have regular communication and interaction with employees will help to engage them in the transition process. They should offer incentives and recognition for adopting new technologies and processes.

*Effective Cost Management.* The commercial banks should strike a balance between cost and quality, optimize investment in electronic banking systems. They should consider cost-sharing options with partners and stakeholders.

By applying these enhancements, commercial banks can dramatically improve their electronic banking security procedures, delivering a secure and efficient banking experience for both consumers and employees.

**References**


[1] Anderson, R. (2020). The importance of regulatory compliance in the banking sector. *Journal of Financial Regulation, 12(1*), 45-59.

[2] Archon S. (2022). Cyber threats in the banking industry. https://www.archonsecure.com/blog/banking-industry-cyber-threats

[3] Bangko Sentral ng Pilipinas. (2020). Regulatory Framework for Cybersecurity in the Philippine Banking Sector. Retrieved from https://www.bsp.gov.ph/regulations/guidelines/

[4] Bangko Sentral ng Pilipinas. (2023). Cybersecurity Guidelines for Electronic Payment Systems in the Philippines. Retrieved from https://www.bsp.gov.ph/regulations/guidelines/

[5] Bowcut, S. (2023). Financial Industry Cybersecurity: Safeguarding assets and data. Cybersecurity Guide. https://cybersecurityguide.org/industries/financial/

[6] Capistrano, E.P. (2021). Trust, acceptance, and use of online banking services in the Philippines. Bangko Sentral ng Pilipinas Professorial Chair Lecture.

[7] Clements, J. (2023). Cyber security in the banking industry - Top trends to know. Managed Outsource Solutions. https://www.managedoutsource.com/blog/cyber-security-in-banking-industry-top-trends-to-know/

[8] De Jesus, M. (2019). 10 online services to try for a cashless existence. SPOT.PH. https://www.spot.ph/newsfeatures/the-latest-newsfeatures/79881/online-bank-wallet-services-guide-philippines-a4362- 20191125-lfrm2

[9] Dela Cruz, M. N., & Reyes, L. S. (2022). Customer Perception of Security in Electronic Banking: A Study of User Behavior in the Philippines. *Journal of Information Security and Privacy*, 39(4), 534-551.

[10] Diokno, B. E. (2020). Benjamin E Diokno: Philippine banking system - forging path towards sustainable economic recovery. https://www.bis.org/review/r201005c.htm

[11] Dusan, L. (2019). DIGITAL BANKING CHALLENGES AND OPPORTUNITIES IN INDIA. *EPRA International Journal of Economic and Business Review*, 20–23. https://doi.org/10.36713/epra2985

[12] Garcia, M. R., & Reyes, L. S. (2019). Investment in Cybersecurity Technology: A Comparative Study of Selected Philippine Commercial Banks. *International Journal of Information Security*, 35(2), 301-318.

[13] Gomez, P. A., & Tan, R. P. (2018). The Role of Artificial Intelligence in Cybersecurity: Case Studies from the Banking Industry. *International Journal of Advanced Computer Science and Applications*, 11(3), 124-139.

[14] Gulyas, O. & Kiss, G. (2022). Cybersecurity threats in the banking sector. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9804140

[15] Hosseini, M., Shajari, S., & Akbarabadi, M. (2022). Identifying multi-channel value co-creator groups in the banking industry. *Journal of Retailing and Consumer Services*, 65, 102312. https://doi.org/10.1016/j.jretconser.2020.102312

[16] Johnson, M. E., Goetz, E. O., & Pfleeger, S. L. (2018). Security through information risk management. Communications of the ACM, 55(3), 58-64.

[17] Kiljan, S., Vranken, H., & Van Eekelen, M. (2018). Evaluation of transaction authentication methods for online banking. Future Generation Computer Systems, 80, 430–447. https://doi.org/10.1016/j.future.2016.05.024

[18] Lim, S. (2020). Continuous Monitoring and Risk Assessment in Cybersecurity: A Framework for Philippine Banks. *International Journal of Cybersecurity Management*, 17(2), 201-220.

[19] Lim, S., & Garcia, M. R. (2019). Multi-Factor Authentication in Electronic Banking: Comparative Analysis of Security Measures. *Journal of Financial Technology*, 27(1), 56-72.

[20] Manila Standard. (2020). How banks and financial institutions can 'get the edge' with technology. Manila Standard. https://manilastandard.net/tech/tech-news/340437/how-banks-and-financial-institutions-can-get-the-edge-with technology.html

[21] Nicolay, R. (2023). Keeping ahead of cybersecurity challenges in financial services. Microsoft Industry Blogs. https://www.microsoft.com/en us/industry/blog/financial-services/2018/10/24/keeping-ahead-ofcybersecurity- challenges-in-financial-services/

[22] Philippine National Privacy Commission. (2021). Data Privacy Regulations Impact on Electronic Banking: Compliance Challenges and Strategies. Retrieved from https://privacy.gov.ph/

[23] Reyes, L. S., & Gomez, P. A. (2023). Incident Response Mechanisms in Electronic Banking Operations: A Comparative Analysis. *Journal of Cybersecurity Research*, 41(1), 78-94.
[24] Reyes, L. S., & Villanueva, C. J. (2021). Emerging Cyber Threats in Electronic Banking: A Risk Assessment Study in Philippine Banks. *Journal of Cybersecurity and Information Assurance*, 37(2), 213-229.
[25] Santos, A. (2021). Enhancing Employee Training and Awareness in Cybersecurity: Best Practices in Philippine Commercial Banks. *Journal of Information Technology Management*, 28(4), 92-107.
[26] Santos, A., & Dela Cruz, M. N. (2020). Security Awareness Campaigns in Philippine Commercial Banks: Impact and Best Practices. *Journal of Information Security Education*, 29(4), 345-360.
[27] Sheeba, A. M., Kumar, M. K., & Raj, P. A. (2023). ELECTRONIC BANKING SERVICES AND AWARENESS: A STUDY. *Journal of Research Administration*, 5(2), 5727-5734. https://journalra.org/index.php/jra/article/view/703
[28] Singh R. R. & Kaur, N. (2019). Interaction between Online Banking and its Impact on Financial Performance of Banking Sector:- Evidence from Indian Public Sector Banks. *International Journal of Recent Technology and Engineering, 8(*2S11), 836–839. https://doi.org/10.35940/ijrte.b1137.0982s1119
[29] Smith, J. (2022). Cybersecurity Challenges in the Banking Sector. *Journal of Banking and Finance*, 46(5), 1125-1138.
[30] Smith, T., & Jones, L. (2018). Enhancing cybersecurity in the financial sector through training and awareness. *Journal of Cybersecurity Education*, 6(1), 22-34.
[31] Stefanini Group (2023). Cybersecurity in digital banking: Everything you need to know - Stefanini.https://stefanini.com/en/insights/articles/cybersecurity-in-digital- banking-everything-you-need-to-know
[32] Tan, R. P., & Lim, S. (2018). Collaborative Efforts in Cybersecurity: A Case Study of Banks and Regulatory Bodies in the Philippines. Cybersecurity Review, 12(3), 45-61.
[33] Villanueva, C. J., & Santos, A. (2019). Blockchain Technology as a Cybersecurity Solution for Philippine Commercial Banks. *Information Security Journal*: A Global Perspective, 28(3), 134-149.
[34] Williams, P., & Parker, S. (2019). Building a culture of cybersecurity in the financial sector. *Journal of Financial Services Security,* 12(3), 15-29.