FINANCIAL TECHNOLOGY AND CYBERSECURITY IN COMMERCIAL BANK IN NEPAL

A Dissertation submitted to the Office of the Dean, Faculty of Management in partial fulfillment of requirement for the Master's Degree

By

Susma Khatiwada

Exam Roll No.: 6417/18

Campus Roll No.: 446/074

TU Registration No.: 7-2-396-137-2013

Shanker Dev Campus

Kathmandu, Nepal

July, 2024

CERTIFICATION OF AUTHORSHIP

I hereby corroborate that I have researched and submitted the final draft of dissertation entitled "**FINANCIAL TECHNOLOGY AND CYBERSECURITY IN COMMERCIAL BANK IN NEPAL**". The work of this dissertation has not been submitted previously for the purpose of conferral of any degrees nor it has been proposed and presented as part of requirements for any other academic purposes.

The assistance and cooperation that I have received during this research work has been acknowledged. In addition, I declare that all information sources and literature used are cited in the reference section of the dissertation.

Susma Khatiwada

Date:

REPORT OF RESEARCH COMMITTEE

Mrs. Susma Khatiwada has defended research proposal entitled **"FINANCIAL TECHNOLOGY AND CYBERSECURITY IN COMMERCIAL BANK IN NEPAL"** successfully. The research committee has registered the dissertation for further progress. It is recommended to carry out the work as per suggestions and guidance of supervisor Rishi Ram Pantha and Dr. Dipak Mahat, and submit the thesis for evaluation and viva voce examination.

…….

Rishi Ram Pantha

Dissertation Supervisor

Dissertation Proposal Defended Date:

…….

……..

Dr. Dipak Mahat

Dissertation Supervisor

Dissertation Submitted Date:

……..

……..

Asso. Prof. Dr. Sajeeb Kumar Shrestha

Position: Research Department

Dissertation Viva-Voce Date:

……

APPROVAL SHEET

We have examined the dissertation entitled "**FINANCIAL TECHNOLOGY AND CYBERSECURITY IN COMMERCIAL BANK IN NEPAL"** presented by Susma Khatiwada for the degree of Master of Business Studies. We hereby certify that the dissertation is acceptable for the award of degree.

……

Rishi Ram Pantha

Dissertation Supervisor

……

Dr. Dipak Mahat
Dissertation Supervisor

……

Internal Examiner

……
Internal Expert

……..

External Expert

……
Asso. Prof. Dr. Sajeeb Kumar Shrestha
Chairperson, Research Committee

……

Asso. Prof. Dr. Krishna Prasad Acharya

Campus Chief

ACKNOWLEDGEMENTS

I extend my heartfelt appreciation to my supervisor, Rishi Ram Pantha and Dr. Dipak Mahat, whose unwavering guidance, continuous motivation, and insightful support were instrumental throughout this project. His expertise profoundly influenced the outcome, and I am deeply thankful for his invaluable assistance and mentorship. Additionally, I wish to express my gratitude to Asso. Prof. Dr. Sajeeb Kumar Shrestha, Chairperson of the Research Committee, and Asso. Prof. Dr. Krishna Prasad Acharya, Campus Chief, along with the entire academic and administrative staff at Shanker Dev Campus. Their unwavering commitment created an environment conducive to learning and personal development, greatly enriching my academic journey and shaping my growth as a scholar.

I am profoundly grateful to my family for their unwavering love, support, and encouragement, which served as the cornerstone of my efforts. Their belief in my abilities and unwavering support fueled my determination to succeed, and I am deeply indebted to them for their sacrifices and encouragement. Furthermore, I acknowledge the invaluable support and camaraderie of my friends and colleagues, whose encouragement and contributions were crucial in overcoming challenges and achieving milestones throughout this journey.

To everyone who contributed to this endeavor, whether through sacrifices, encouragement, or belief in my abilities, I express my sincerest gratitude. Your support was pivotal to the successful completion of my dissertation, and I am truly grateful for the opportunity to embark on this academic journey with your unwavering support and guidance.

Susma Khatiwada

TABLE OF CONTENTS

LIST OF TABLES

Tables **Page**

LIST OF FIGURE

Figure **Page**

ABBREVIATIONS

AI	:	Artificial Intelligence
ANOVA	:	Analysis of Variances
CAS	:	Competence and Skill
CGAR	:	Compound Annual Growth Rate
CYS	:	Cyber Security
DMB	:	Deposit Money Banks
E	:	Error Term
Fintech	:	Financial Technology
FTPs	:	Fintech Products
GFC	:	Global Financial Center
INS	:	Information Security
N	:	Number of Responses
NRB	:	Nepal Rastra Bank
S.D.	:	Standard Deviation
SEF	:	Self-Efficacy
TEC	:	Technological Culture
USD	:	United States Doller

ABSTRACT

This study evaluates the impact of financial technology (Fintech) on cybersecurity in commercial banks in Nepal, aiming to address the challenges posed by the digitization of financial services. By analyzing the relationship between Fintech adoption and cybersecurity measures, the study seeks to identify potential risks and vulnerabilities while assessing the overall impact of financial technology on commercial banks in Nepal.

The research design encompasses a descriptive and causal-comparative approach, targeting employees in commercial banks within the Kathmandu Valley, Nepal. A sample size of 385 participants is selected using convenience sampling, drawn from various types of banks. Data collection is conducted through structured questionnaire surveys to capture relevant variables and factors identified in the literature, employing a five-point Likert scale for measurement.

Statistical software such as Microsoft Excel and SPSS are utilized for data analysis, employing descriptive statistics, correlation analysis, and multivariate regression models. These analytical tools allow for the exploration of the relationship between Fintech adoption and cybersecurity measures, controlling for other relevant factors outlined in the research framework.

The findings reveal that independent variables such as self-efficacy, information security, technological culture, and competence and skill collectively serve as significant determinants of cybersecurity readiness in commercial banks in Nepal. The regression analysis indicates a positive impact of each independent variable on cybersecurity, emphasizing the importance of organizational culture and employee empowerment in addressing cybersecurity challenges effectively.

Practically, the study underscores the importance of enhancing cybersecurity measures in commercial banks, especially in light of increasing Fintech adoption. Theoretical implications contribute to understanding the complex dynamics between Fintech and cybersecurity readiness. Recommendations include implementing robust cybersecurity protocols, fostering a culture of cybersecurity awareness, and investing in continuous training and education for employees to mitigate cyber threats effectively.

Keywords: *Financial technology, cybersecurity, Fintech adoption, Self-efficacy, Information security*

CHAPTER I
INTRODUCTION

1.1 Background of the Study

Financial technology, commonly known as Fintech, represents a transformative force in the financial services industry, leveraging technology to enhance operations and accessibility (Alodhiani et al., 2023). This innovation has led to the emergence of cellular banks, mobile investing services, and digital currencies like Bitcoin, revolutionizing how financial services are delivered and accessed globally. Start-ups, incumbent banks, and IT firms collaborate within the Fintech sector to improve or replace traditional financial services, driving efficiency and expanding market reach (Stanciu & Tinca, 2017).

As Peters et al., (2015) note, modern financial institutions increasingly adopt Fintech solutions to advance service offerings and bolster market competitiveness. This trend underscores the pivotal role of technology in reshaping financial landscapes and driving economic growth. However, alongside its benefits, the proliferation of Fintech introduces new challenges, particularly in cybersecurity. The rapid digitization of financial services amplifies the risk of cyber-attacks, threatening the stability of financial systems and the security of consumer data (Jasur, 2023).

The intersection of financial technology and cybersecurity necessitates a nuanced approach to risk management and regulatory oversight. Policymakers, industry stakeholders, and regulatory bodies play a crucial role in establishing frameworks to safeguard against cyber threats while fostering innovation. Philippon (2016) and Shah et al., (2018) emphasize the importance of regulatory measures to mitigate risks and ensure the resilience of financial ecosystems in the face of evolving cyber threats.

The evolution of financial technology over the past decade has democratized access to financial services, empowering consumers with unprecedented convenience and choice. However, this democratization comes with inherent risks, particularly concerning the security of personal information and the potential misuse of emerging technologies like machine learning and artificial intelligence for malicious purposes (Al-Duhaidahawi et al., 2019). The challenge lies in balancing innovation and security to protect consumers without stifling technological advancement.

Nonetheless, the rapid expansion of Fintech, including the proliferation of online lending platforms and payment processing services, necessitates robust regulatory oversight to safeguard consumer interests. Alshehadeh and Al-Khawaja (2022) highlight the role of industry watchdogs in ensuring compliance with standards and implementing essential security measures to mitigate risks associated with electronic financial services. Moreover, the rise of cryptocurrencies introduces novel challenges, such as concerns regarding money laundering and consumer safety, necessitating regulatory interventions to address emerging threats (Firmansyah & Anwar, 2019; Al-Duhaidahawi et al., 2019).

Overall, the convergence of financial technology and cybersecurity presents both opportunities and challenges for the financial services industry. While Fintech innovations drive efficiency and expand access to financial services, they also heighten the risk of cyber threats and financial misconduct. Addressing these challenges requires a collaborative effort among stakeholders to develop robust regulatory frameworks, enhance cybersecurity measures, and promote responsible innovation. By striking a balance between innovation and security, the financial industry can harness the full potential of Fintech while safeguarding the integrity and resilience of financial ecosystems.

This study primarily focused on the introduction of financial technology (Fintech) and its impact on the cybersecurity landscape of commercial banks in Nepal. As Fintech continues to gain traction in the country, transforming traditional banking practices and enhancing financial services accessibility, it also poses new challenges in terms of cybersecurity. This research aims to analyze the implications of Fintech adoption on the cybersecurity posture of commercial banks in Nepal, identifying potential risks and vulnerabilities while exploring strategies to mitigate cyber threats and safeguard financial institutions and their customers in this evolving digital landscape.

1.2 Problem Statement

The burgeoning adoption of financial technology (Fintech) in commercial banks across Nepal presents a double-edged sword, introducing both opportunities and challenges in the realm of cybersecurity (Maharjan & Chatterjee, 2019). As these institutions embrace digital transformation to enhance operational efficiency and customer experience, they become increasingly susceptible to the nefarious activities of cybercriminals. The primary issue lies in the rapid growth and sophistication of financial and banking services

facilitated by Fintech, which inadvertently amplifies the potential risks and vulnerabilities inherent in digital ecosystems (Shrestha, 2020). With the proliferation of online transactions, mobile banking, and digital payment platforms, commercial banks in Nepal face heightened exposure to cyber threats, ranging from data breaches and identity theft to ransomware attacks and fraudulent activities.

Furthermore, the rise of Fintech-enabled services is accompanied by a surge in malicious cyber assaults, posing significant challenges for commercial banks in Nepal. These institutions must contend with the constant threat of cyber-attacks targeting their sensitive financial data, customer information, and digital infrastructure. The evolving nature of cyber threats necessitates proactive measures to fortify cybersecurity defenses and mitigate potential risks to financial stability and customer trust (Giri & Shakya, 2020). However, many commercial banks in Nepal may lack the resources, expertise, and regulatory oversight to adequately address these challenges, leaving them vulnerable to exploitation by cyber adversaries.

In light of these developments, the oversight of financial operations and regulatory authorities assumes paramount importance in safeguarding the integrity and security of commercial banks in Nepal. Effective oversight mechanisms are essential to monitor the evolving landscape of electronic financial processes and mitigate the hazards associated with Fintech adoption (Giri & Shakya, 2020). Regulatory bodies must play a proactive role in setting stringent cybersecurity standards, conducting regular audits, and enforcing compliance measures to ensure that commercial banks adhere to best practices in cybersecurity. Moreover, collaboration between industry stakeholders, government agencies, and cybersecurity experts is crucial to develop comprehensive strategies for mitigating cyber risks and enhancing the resilience of Nepal's financial sector in the face of emerging threats posed by financial technology. The research questions for this study are as follows:

1. What is the current status of cybersecurity in commercial banks in Nepal?
2. Is there any relationship between financial technology and cybersecurity in commercial banks in Nepal?
3. Is there any impact of financial technology and cybersecurity in commercial banks in Nepal?

1.3 Objectives of the Study

The objective of this study are as follows:

1. To assess the current status of cybersecurity in commercial banks in Nepal.
2. To analyze the relationship between financial technology and cybersecurity in commercial banks in Nepal.
3. To examine the impact of financial technology and cybersecurity in commercial banks in Nepal.

1.4 Research Hypothesis

The following research hypothesis have been established and evaluated for empirical verification in order to meet the study's objectives and answer the research questions:

Hypothesis I

H_1: There is a significant positive relationship between self-efficacy and the effectiveness of cybersecurity measures within commercial banks.

Hypothesis II

H_2: There is a significant positive relationship between information security culture and the effectiveness of cybersecurity measures within commercial banks.

Hypothesis III

H_3: There is a significant positive relationship between technological competence and the effectiveness of cybersecurity measures within commercial banks.

Hypothesis IV

H_4: There is a significant positive relationship between skill and the effectiveness of cybersecurity measures within commercial banks.

1.5 Rationale of the Study

The study has significant importance for various stakeholders including commercial banks, government agencies, the Nepal Rastra Bank (NRB), policymakers, researchers, academicians, and students.

- **Commercial Banks:** Commercial banks in Nepal are at the forefront of adopting financial technology (Fintech) solutions to modernize their operations and enhance customer experiences. Understanding the intricacies of cybersecurity

within this evolving landscape is paramount for these banks to safeguard their digital assets, maintain customer trust, and ensure uninterrupted service delivery. By comprehensively analyzing the relationship between Fintech and cybersecurity, commercial banks can develop robust strategies to mitigate risks and strengthen their cyber resilience.

- **Government:** The government of Nepal plays a crucial role in regulating and overseeing the financial sector, including commercial banks. As Fintech adoption accelerates, the government needs to ensure that appropriate regulatory frameworks are in place to address cybersecurity concerns effectively. This study provides valuable insights that can inform policy decisions aimed at promoting innovation while safeguarding the integrity and stability of the financial system.
- **Nepal Rastra Bank (NRB):** As the central bank of Nepal, the NRB plays a pivotal role in supervising and regulating commercial banks to maintain financial stability and consumer protection. Understanding the intersection between financial technology and cybersecurity is essential for the NRB to formulate policies, guidelines, and regulatory frameworks that promote responsible innovation and mitigate systemic risks. This study can assist the NRB in enhancing its oversight mechanisms and strengthening the resilience of the banking sector against cyber threats.
- **Policymakers:** Policymakers in Nepal need to stay abreast of emerging trends in financial technology and cybersecurity to address the evolving challenges facing the banking industry. By gaining insights from this study, policymakers can devise proactive measures to foster a conducive environment for Fintech innovation while addressing cybersecurity risks. Policy interventions informed by empirical research can enhance the competitiveness and sustainability of Nepal's banking sector in the digital age.
- **Researchers and Academicians:** Researchers and academicians play a vital role in advancing knowledge and understanding in the fields of Fintech and cybersecurity. This study provides a foundation for further research and academic inquiry into the nuances of technological innovation and its implications for cybersecurity in commercial banks. By building upon the findings of this study, researchers can contribute to the development of best practices, theoretical

frameworks, and practical solutions to address cybersecurity challenges in the banking sector.

- **Students:** For students pursuing studies in finance, technology, cybersecurity, or related fields, this study offers valuable insights into real-world challenges and opportunities within the banking industry. By engaging with the research findings and methodologies presented in this study, students can deepen their understanding of the complex interplay between financial technology and cybersecurity. Moreover, this study can inspire students to explore career opportunities and research interests in areas such as Fintech regulation, cybersecurity management, and digital banking innovation.

1.6 Limitations of the Study

This study has following limitations.

- Limited availability of primary data due to constraints in accessing relevant information from commercial banks in Nepal.
- Variable constraint, as the study may face limitations in assessing all relevant financial technology and cybersecurity variables within the scope of Nepalese commercial banks.
- Lack of existing research articles specifically focusing on the intersection of financial technology and cybersecurity within the context of commercial banks in Nepal, leading to a scarcity of reference materials.
- The study's exclusive focus on commercial banks may limit its generalizability to other financial institutions or sectors within Nepal's financial industry.

CHAPTER II
LITERATURE REVIEW

This chapter presents a comprehensive literature review. The conceptual review explores foundational concepts and provides a detailed examination of the key ideas related to the study. The theoretical review delves into relevant theories and frameworks that underpin the research. The empirical review analyzes previous studies and research findings in the field. Finally, the research gap identifies areas where further investigation is needed, highlighting the unique contribution of this study.

2.1 Conceptual Review

This section delves into various aspects of the fintech ecosystem. It begins with an exploration of the dynamics and challenges within the fintech ecosystem, providing a foundational understanding of its environment. The review then addresses the relationship between fintech and information security, highlighting critical security concerns. It also differentiates between cybersecurity and information security, providing clarity on these interconnected but distinct concepts. Finally, the review examines cybersecurity within the fintech sector, emphasizing the unique security challenges and solutions specific to fintech.

2.1.1 The Fintech Ecosystem: Dynamics and Challenge

The Fintech market has seen significant growth and geographical expansion, with investment forecasts projecting its evolution from 3 billion to 8 billion USD in 2018. This growth has been fueled by the disruptive nature of Fintech, which challenges traditional financial institutions and forces them to either develop internal capabilities or collaborate to remain competitive. Understanding the Fintech ecosystem is crucial for identifying its dynamics and challenges. Initially proposed by Diemers et al., (2015), the ecosystem involves three key parties: entrepreneurs, governments, and financial institutions. Governments play a role in implementing regulatory environments to support entrepreneurial activity, while financial institutions collaborate with Fintech startups to enhance their competitiveness.

Entrepreneurs drive innovation within the ecosystem by providing disruptive solutions to the financial industry. Building on this model, Lee and Turban (2001) identified two additional participants: technology developers and financial customers. Their model

highlights the competitive dimension between Fintech startups and traditional financial entities. Despite the opportunities presented by Fintech, both financial institutions and Fintech startups face various challenges, including investment management, customer management, regulation, technology integration, security and privacy, and risk management. Among these challenges, regulation and security issues have particularly influenced the technological acceptance of Fintech, emphasizing the interconnectedness of regulatory and security concerns in the Fintech landscape.

The global Fintech market has experienced remarkable growth in recent years, with a valuation of USD 294.74 billion in 2023. Projections indicate further expansion, with the market expected to reach USD 340.10 billion in 2024 and soar to USD 1,152.06 billion by 2032. This trajectory reflects a robust compound annual growth rate (CAGR) of 16.5% during the forecast period from 2024 to 2032. Such substantial growth underscores the increasing adoption of Fintech solutions across various sectors and regions worldwide. Factors such as technological advancements, changing consumer preferences, and regulatory developments contribute to the expanding scope and significance of the Fintech market on a global scale. As Fintech continues to revolutionize financial services and reshape industry landscapes, stakeholders must adapt to evolving trends and seize opportunities for innovation and collaboration in this dynamic ecosystem (Alt et al., 2024).

2.1.2 Fintech and Information Security

The surge of the Fintech industry has been propelled by a changing regulatory landscape, thrusting the sector into the spotlight. However, this regulatory spotlight also highlights a significant challenge inherent to Fintech: information security. Given the nature of their business operations, Fintech companies must place paramount importance on information security. Firstly, Fintechs enter the financial sector as non-traditional service providers, necessitating a robust approach to safeguarding sensitive data and transactions (Kryparos, 2018). Secondly, the very business model of Fintechs revolves around the concept of being "always available," which presents a fundamental tension between availability and security. While promising uninterrupted service, Fintechs must also ensure stringent security measures to protect against cyber threats.

Traditionally, achieving security through obscurity was a common strategy, relying on isolation and limited access. However, in today's interconnected digital landscape

dominated by open networks and web technologies, this approach has become increasingly obsolete (Kryparos, 2018). Fintechs fully embrace these digital features to offer innovative solutions that cater to customer needs overlooked by traditional financial institutions. Yet, this emphasis on customer-centricity shifts attention away from ensuring a delicate balance between availability and security, posing a formidable challenge.

Moreover, the pressure to expedite time-to-market within the Fintech ecosystem often leads to a race against time, where cutting corners becomes tempting (Kryparos, 2018). This rush to market may result in launching products or services without adequate security measures in place, jeopardizing the company's integrity and future viability. The analogy drawn between information security and racing cars underscores the essential role of security measures in ensuring sustainability, akin to brakes enabling speed in a racing car.

In response to the need for rapid software development, agile methodologies like the Agile Manifesto have gained popularity. While aiming to enhance collaboration and speed in software development, these methodologies often prioritize frequent delivery intervals and customer needs over broader considerations such as sustainability and security (Kryparos, 2018). Consequently, technical vulnerabilities may arise, requiring frequent software updates and undermining public confidence in the technology's reliability.

The repercussions of launching non-robust solutions into the market extend beyond immediate credibility loss, potentially damaging brand reputation and accumulating technical debt for the company (Kryparos, 2018). This technical debt, akin to building a house on sand, compounds over time, posing significant challenges for future software development efforts. Thus, the urgency to address the intricate interplay between availability, security, and speed underscores the imperative of studying information security within the Fintech domain comprehensively.

2.1.3 Cybersecurity and Information Security

In recent years, cybercriminal activities have garnered significant attention globally, driven by high-profile incidents that underscore the critical need for robust security measures. This heightened focus has sparked debates surrounding the definitions and distinctions between cybersecurity and information security. Von Solms and Von Solms

(2018) delve into this discourse, aiming to shed light on the commonalities and delineations between these terms.

Further elucidating the relationship, Von Solms and Von Solms (2018) highlight the comprehensive scope of information security, which encompasses all forms of information, contrasting with cybersecurity's focus on safeguarding digital assets. This distinction underscores cybersecurity's role in protecting interconnected networks and digital information assets within cyberspace. This nuanced understanding is encapsulated in their graphical representation, where cybersecurity is depicted as a component of information security.

While these definitions provide a foundational understanding of cybersecurity and information security governance, their application within specific contexts, such as the Fintech industry, requires further exploration. Consequently, the subsequent section will delve into the multifaceted forms that cybersecurity assumes within the Fintech landscape, elucidating its implications and governance frameworks tailored to address industry-specific challenges and risks.

2.1.4 Cybersecurity Within Fintech

In their exploration of cybersecurity within the Fintech domain, Gai et al., (2018) offer insights into the multifaceted challenges faced by financial technology firms. A primary concern highlighted by the authors revolves around security and privacy issues, which are categorized into three dimensions: business operations, outsourcing, and financial privacy. Traditionally, security matters were confined to the realm of business operations within the financial industry. However, the landscape has evolved, with incidents shedding light on the complexities involved in analyzing and interpreting security breaches to formulate effective strategies (Gai et al., 2018). Despite the intricacies, it is evident that securing electronic transactions hinges on addressing privacy concerns and establishing robust trust mechanisms.

The quest to establish trust mechanisms prompts an examination of practical cybersecurity dimensions. Drawing from the work of Von Solms & Von Solms (2018), cybersecurity is primarily associated with internetworked information systems, commonly understood as the Internet. Expanding this notion, particularly within the Fintech context, involves encompassing the Internet of Things (IoT), reflecting the interconnected nature of digital ecosystems (Gai et al., 2018). Within this framework, Gai

et al., (2018) propose two avenues for mitigating security risks and fostering trust: physical methods and application-based solutions.

Gai et al., (2018) advocate for the development and implementation of both physical and application-based approaches to address security risks effectively. Physical methods may involve robust infrastructure and hardware solutions to safeguard electronic transactions and sensitive data. On the other hand, application-based methods leverage software solutions and encryption techniques to fortify digital platforms against cyber threats (Gai et al., 2018). The integration of these methods aims to instill confidence among stakeholders and users, thereby bolstering trust in Fintech platforms.

As Fintech continues to reshape the financial landscape, the imperative to prioritize cybersecurity measures becomes increasingly pronounced. The convergence of physical and digital security measures underscores the multifaceted nature of cybersecurity within the Fintech domain. By embracing both physical and application-based solutions, financial technology firms can navigate security challenges and cultivate trust in their platforms, fostering a conducive environment for innovation and growth in the Fintech sector.

2.2 Theoretical Review

This section presents an in-depth theoretical review, beginning with systems theory, which provides a framework for understanding the complex interactions within the fintech ecosystem. It then explores personality theory, examining how individual traits and behaviors influence security practices. The review continues with risk expectations theory, which discusses the role of perceived risks in shaping user and institutional responses to security threats. Finally, institutional theory is considered, highlighting how organizational structures and norms impact the implementation and effectiveness of cybersecurity measures.

2.2.1 Systems Theory

Systems theory, rooted in the idea that the whole is greater than the sum of its parts, provides a conceptual framework for understanding complex systems by emphasizing the relationships between their components rather than viewing them in isolation. According to Gaur et al., (2023), systems theory posits that the parts of a system can best be understood in terms of their interactions with each other and with other systems. In the context of cybersecurity, which comprises multiple interconnected components,

addressing its challenges necessitates an approach that considers all individual elements comprehensively. Gaur et al., (2023) outlines five basic concepts of systems theory: systems, elements, relationships, the universe, and the environment. Systems represent distinct elements within the total reality, while elements are the minor parts required for systematic analysis. Relationships describe the dependencies between elements, and the universe encompasses all elements and their relationships, known and unknown. The environment comprises any part of the universe with direct relationships with the elements within the system.

Applying systems theory, specifically systems thinking, to cybersecurity involves understanding the relationships between components and their collective impact on the system. Amissah et al., (2019) describe systems thinking as an approach to reasoning and problem-solving based on understanding these relationships and their intentional or unintentional effects on the system as a whole. In cybersecurity, Savage and Schneider (2009) assert that security is a holistic problem, where even minor changes to system elements can have significant consequences for security. Cybersecurity encompasses various aspects, including people, processes, and technology, each comprising multiple minor elements.

The characteristics of cybersecurity, as identified by Salim (2014), include complexity, unpredictability, dynamism, and asymmetry. Systems thinking can help bridge the gap between different domains involved in cybersecurity decision-making, such as social, technical, economic, regulatory, legislative, and political aspects. This approach aligns with the trifold approach to cybersecurity, which emphasizes the contributions of people, processes, and technology to the overall security posture. However, the success of systems thinking depends on the interaction and interdependence of elements, which can be hindered by organizational silos and resistance to change within large organizations like banks. Additionally, while systems thinking emphasizes adaptability, it may not address the need for certain elements to be changed to align with the organization's overall vision, posing a challenge to its implementation in cybersecurity contexts.

2.2.2 Personality Theory

Personality theory, as it relates to trust, focuses on interpreting trust from a psychological perspective. According to Lee and Turban (2001), this perspective places the individual and their attributes at the center of the trust construct, suggesting that trust originates from

the individual's personality. In essence, trust is viewed as a psychological state that can be influenced by various factors in the environment, as well as by the individual's beliefs, values, and emotions (Beldad et al., 2010). This theory posits that individuals may have different propensities to trust, which are shaped by their personality traits and their unique developmental experiences, as well as by their cultural background.

Within the framework of personality theory, trust is seen as a complex interplay between individual characteristics and external influences. Individuals may exhibit varying levels of trust based on their personality traits, such as openness, agreeableness, and conscientiousness. Additionally, their past experiences, cultural upbringing, and social environment can shape their attitudes toward trust. For example, individuals who have experienced betrayal or deception in the past may have lower levels of trust compared to those who have had positive and trusting relationships (Beldad et al., 2010). Similarly, cultural norms and values can influence how individuals perceive and approach trust, with some cultures placing greater emphasis on collective trust and others on individual autonomy.

Overall, personality theory offers valuable insights into the psychological underpinnings of trust. By understanding how personality traits, experiences, and cultural factors influence trust, researchers and practitioners can gain a deeper understanding of how trust operates in various contexts and how it can be nurtured or restored in interpersonal relationships and organizational settings (Beldad et al., 2010).

2.2.3 Risk Expectations theory

The second perspective explored in the literature views trust as an expectation, emphasizing its sociological function rather than its psychological underpinnings. According to Williams and Findlay (1986), trust plays a crucial role in establishing and maintaining social relationships, contributing to stability through the exchange of obligations. From this viewpoint, trust is understood both psychologically and sociologically, shaping individuals' expectations in interactions. Roush (2007) delineates three types of expectations resulting from trust: the expectation of social order maintenance, the expectation of competent role performance, and the expectation of fulfilling economic and moral obligations.

This perspective shifts the focus to the relationship between the trustor and trustee, questioning the trustor's perception of the trustee's honesty and integrity in fulfilling their

intended role, regardless of the material outcome. Here lies a paradox: the trustor projects trustworthiness onto the trustee, yet trusts are partly assessed by the trustor's ability to evaluate the reliability of the trustee (Roush, 2007). Trust, viewed transactionally, encompasses dimensions such as reputation, performance, and appearance.

Additionally, this perspective introduces the concept of vulnerability inherent in trust. Zand (1972) suggests that trusting individuals relinquish some power to the other party, increasing their vulnerability by placing themselves in situations they cannot fully control. Trust implicitly involves accepting the risk of vulnerability, as uncertainties underlie all exchanges (Wu & Liu, 2022). This raises a fundamental question: does one trust because of the exposure to risk, or does one take risks because of trust? The former implies that risks determine trust, while the latter suggests that trust precedes risk-taking behaviors. This dilemma underscores the complexity of trust and whether participants act rationally or irrationally within trust interactions.

2.2.4 Institutional Theory

The final perspective on trust arises from considering both sociological and economic implications. Within this framework, trust is viewed collectively rather than as an individual phenomenon. This collective perspective allows trust to be applied to relationships among individuals, focusing on social interactions grounded in the exchange of goods, whether material or immaterial. While social exchange is primarily driven by individuals seeking a voluntary relationship based on expected returns, these returns are often undefined, distinguishing social exchanges from economic ones, which typically involve formal contracts (Amenta & Ramsey, 2010). Despite this difference, trust is essential for both types of exchanges to continue or be completed. Moreover, trust within social exchanges highlights the dependency between actors, as individuals may rely on others to meet their needs, with commitment between parties contingent on trust.

Another aspect highlighted by viewing trust from both sociological and economic perspectives is its collective nature. Trust is no longer confined to describing individual interpersonal exchanges but extends to interactions with groups, organizations, or institutions (Amenta & Ramsey, 2010). Thus, trust can be defined as the reliance of one party on an established duty ensured by another party, aimed at protecting and acknowledging the rights and interests of all parties involved. This conceptualization

broadens the scope of trust interactions, emphasizing its role in various social and economic contexts beyond individual relationships.

2.3 Empirical Review

Samoei and Gatobu (2024) conducted a study aiming to assess the impact of cybersecurity on the performance of internet banking services in commercial banks within Nairobi City County, Kenya. Employing a descriptive research design, the study encompassed all 38 licensed commercial banks in the county, utilizing a structured questionnaire to collect primary data. Statistical analysis was conducted using the Statistical Software for Social Sciences (SPSS), with results presented in tabular form. The study found that application security significantly influences the performance of internet banking services, indicating the importance of safeguarding customer information and funds from cyber threats. Additionally, IT governance emerged as another crucial determinant, suggesting the necessity for professional and dedicated teams to enhance trust, customer satisfaction, and competitiveness. Based on these findings, the study recommends that commercial banks enhance the security of their mobile banking applications by incorporating more person-specific security features, such as fingerprints and two-factor authentication (2FA) codes, to mitigate cyber risks effectively. Furthermore, it emphasizes the importance of bolstering IT governance practices to ensure robust cybersecurity measures are in place, thereby safeguarding the integrity and reliability of internet banking services in the face of evolving cyber threats.

Umoga et al., (2024) conducted a critical review of emerging cybersecurity threats in financial technologies. The main objective of their study was to analyze the challenges and vulnerabilities faced by financial institutions amidst the rapid evolution of financial technologies. Employing a literature review approach, the researchers synthesized existing research to explore the spectrum of cyber threats, ranging from traditional phishing and malware attacks to sophisticated ransomware and supply chain attacks. They assessed the impact of regulatory frameworks and compliance measures on mitigating cybersecurity risks in the Fintech domain, evaluating the effectiveness of current strategies and suggesting potential enhancements. Additionally, the study focused on human factors in cybersecurity, emphasizing the importance of robust training and awareness programs to address social engineering attacks, insider threats, and human vulnerabilities. The major findings of the study underscored the interconnectedness of Fintech platforms, the need for proactive and adaptive cybersecurity strategies, and the

imperative of safeguarding the integrity and security of financial technologies in the face of evolving cyber threats.

Alsakini et al., (2024) investigated the impact of cybersecurity breaches on the quality of financial accounting statements in selected banks in Jordan. Their study aimed to assess how cybersecurity incidents, such as accidental information disclosure (ADID), stealing the encryption key (STEK), malicious internal opening access (MVIA), database breach (DTBB), man-in-the-middle attacks (MITM), malware with encryption (MWWE), and malicious external attacks (MVEA), affect the balance sheet, cash flow statement, and profit and loss accounting. The researchers utilized two datasets and sampling approaches: primary data consisting of 506 data points on cybersecurity breaches from 2012 to 2022 and secondary data collected through a survey of 170 participants. Their findings revealed that cybersecurity breaches significantly impacted the quality of financial accounting statements. Specifically, breaches like ADID, STEK, DTBB, MITM, MWWE, and MVEA were found to have significant effects on various aspects of financial statements. However, MVIA did not demonstrate a significant impact. The study underscores the importance of rapid response to cyberattacks to mitigate their adverse effects on a bank's financial statements and reputation. Overall, the research provides valuable insights into the intricate relationship between cybersecurity and the quality of financial accounting statements in the banking sector, emphasizing the imperative for robust cybersecurity measures to safeguard financial information.

Farayola (2024) proposed a methodology to revolutionize banking security by integrating Artificial Intelligence (AI), Blockchain, and Business Intelligence (BI) for enhanced cybersecurity. The study aimed to address the pressing need for innovative solutions in the dynamic landscape of banking security, particularly in the face of evolving cyber threats. Traditional security approaches have been reactive and struggle to keep pace with cybercriminal tactics, necessitating proactive defense mechanisms. AI offers a proactive defense by analyzing vast amounts of data to identify patterns indicative of suspicious behavior, enabling swift detection and mitigation of security breaches. Blockchain technology introduces a decentralized and immutable ledger, enhancing the security and transparency of transactions while reducing the risk of fraud and unauthorized access. Additionally, Blockchain facilitates secure data sharing among stakeholders, promoting collaboration while maintaining data integrity. Complementing AI and Blockchain, BI provides actionable insights derived from data analytics, enabling banks to gain a deeper

understanding of their security posture and prioritize remediation efforts. The study highlights the potential of integrating AI, Blockchain, and BI to revolutionize banking security, offering a paradigm shift towards a resilient financial ecosystem.

Choithani et al., (2024) conducted a comprehensive study focusing on the intersection of artificial intelligence (AI), cybersecurity, Bitcoin, cryptocurrency, and the banking system. The primary objective was to explore the role of AI techniques in addressing various aspects related to cryptocurrencies, including risk reduction, price prediction, trend analysis, portfolio construction, and fraud detection. The study reviewed recent research in the field, particularly emphasizing AI and machine learning (ML) techniques such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU). By synthesizing relevant literature, the paper identified key research opportunities and areas for enhancing the efficiency of AI-based approaches in cryptocurrency analysis and management. Furthermore, the study highlighted the rapid advancement of AI and its significant impact on finance, markets, institutions, and legislation. It underscored the transformative potential of AI in streamlining financial processes, improving customer services, and revolutionizing the banking sector. Specifically, the research discussed the adoption of AI by Indian banks, such as RBI, SBI, and HDFC, to digitally enhance customer experiences through chatbots and other AI-driven solutions. Overall, the study contributed to understanding the multifaceted implications of AI and cybersecurity in the context of Bitcoin, cryptocurrency, and the banking industry, while also offering insights into future research directions and practical applications in the financial domain.

Gholami et al., (2023) undertook a descriptive-analytical study to delve into the factors influencing the integration of Fintech within Iran's banking sector. Their research aimed to provide comprehensive solutions for overcoming obstacles and fostering growth in the industry by grasping the present circumstances. Data collection involved library studies and questionnaires distributed to a sizable sample of 12,147 bank personnel in Iran during the year 1400. To ensure a representative sample, Cochran's method and random sampling were employed. Through structural equation modeling using Smart PLS statistical software, the researchers tested main and sub-hypotheses derived from their investigation. Results confirmed the primary hypothesis and its subsidiary counterparts, highlighting the necessity for aligning with existing legal frameworks and enhancing infrastructure to facilitate the implementation of Fintech strategies in Iran's banking

landscape. The study emphasized key objectives such as promoting transparency, reducing operational costs, delivering expedited services, and transitioning towards a smarter economy within the banking sector. Overall, the research contributes valuable insights into the essential factors driving the adoption of Fintech in Iran's banking sector and suggests potential avenues for future advancement and development.

Dung et al., (2023) explored the application of financial technology (Fintech) in commercial banks, aiming to understand its current state and propose solutions to enhance its efficiency. The study delved into how advancements in information technology and the internet have transformed consumer behaviors and operational paradigms within commercial banking. Fintech applications have permeated various facets of banking, including deposits, payments, insurance, securities, credit, and risk management, consequently reshaping market structures and long-term development plans of banks. The research design likely involved a thorough examination of existing literature, along with potentially conducting surveys or interviews with banking professionals to gather insights into the current state of Fintech adoption in commercial banks. Major findings of the study would include an assessment of the current landscape of Fintech utilization in commercial banking, identifying challenges or inefficiencies, and proposing solutions to address them. Overall, the study underscores the significant influence of Fintech on the banking industry and emphasizes the need for strategic solutions to optimize its application for enhancing operational efficiency and customer service in commercial banks.

Despotović et al., (2023) conducted a comprehensive analysis of cybercrime and cybersecurity in the field of financial technologies (Fintech), aiming to address the evolving threats and vulnerabilities associated with the digital transformation of the financial industry. The study utilized a systematic approach to identify and describe the threats and dangers of cybercrime in Fintech, analyzing modern ways of protecting financial systems from such threats. By defining and explaining how cyber-attacks manifest themselves and how they can be prevented, the researchers underscored the importance of user awareness and employee training in mitigating potential risks. The paper explored various types of cyber-attacks in detail and emphasized the necessity of considering cyber risks in detail to provide an adequate counter-response to each element. Furthermore, the authors delved into the vulnerabilities of financial systems, the adaptation of cyber-attacks to modern business, and the impact of cryptocurrencies on

financial operations and cybercrime. Through a systematic analysis, the study culminated in a list of recommendations for various stakeholders, including banks, Fintech companies, and end users, to enhance cybersecurity measures and mitigate cyber threats effectively. The findings contribute to the understanding of cybersecurity challenges in the context of Fintech and provide valuable insights for developing strategies to safeguard financial systems in the digital era.

Akintoye et al., (2022) conducted a study on the impact of cybersecurity on the financial innovation of selected Deposit Money Banks (DMBs) in Nigeria. The research aimed to address the pressing need for financial innovation in DMBs, driven by population growth and the challenge of reducing financial exclusion. Utilizing a survey research design, the study collected primary data through structured questionnaires administered to fifty-six senior staff members from key impacted departments of DMBs, representing 93% of the total market capitalization as of December 31, 2021. The analysis of the collected data, employing descriptive and inferential statistics, revealed a statistically significant positive impact of cybersecurity, as proxied by risk management and bank monitoring, on the financial innovation of DMBs in Nigeria. The study's findings highlighted the importance of regular review, revision, and strengthening of risk management frameworks to address emerging challenges from the deployment of financial innovation products and services. Additionally, the study recommended enhancing the monitoring of e-banking channels to facilitate greater reliance on them for financial transactions. Overall, the research shed light on the critical role of cybersecurity in driving financial innovation in DMBs and provided actionable recommendations for improving risk management practices and enhancing the security of e-banking channels in Nigeria's banking sector.

Șcheau et al., (2022) conducted a study focusing on the key pillars for Fintech and cybersecurity in response to the rapid digitalization of financial services and the increasing complexity of cyber threats. The main objective was to address the need for responsible cybersecurity policies and regulations to accompany the technological advancements adopted by financial technology companies. The researchers emphasized the importance of leveraging advancements in fields such as data analytics, artificial intelligence, and blockchain technology to meet the evolving customer needs in the digital era. They argued that as the financial sector embraces digitalization, the protection of customer data becomes more complex due to the proliferation of cyber-attack vectors. The study provided an overview of the growing intensity of cybercrime in the financial

sector and highlighted common cyber threats affecting the industry. Additionally, the researchers emphasized the importance of adopting proactive cybersecurity measures rather than relying solely on reactionary approaches. Overall, the study underscored the urgent need for a comprehensive approach to cybersecurity in the financial services sector, incorporating both technological and human perspectives to mitigate cyber risks effectively.

Vučinić and Luburić (2022) conducted a study focusing on the intersection of financial technology innovations (Fintech), risk-based thinking, and cyber risk in the context of modernizing the financial system. The main objective was to examine the latest developments in Fintech, including its potential benefits and associated risks, and to underscore the vital role of monetary authorities in managing these changes while preserving monetary and financial stability. The authors emphasized the significance of artificial intelligence in driving Fintech development and introduced a Fintech SWOT analysis to support their examination. Furthermore, they introduced the concept of "Risk-based thinking" as a management approach to navigate the opportunities and threats presented by Fintech. A key focus of the study was on cyber risk in the Fintech landscape, identified as a significant and evolving threat arising from the rapid changes in the financial sector. By addressing these themes, the study aimed to provide insights into the policies and initiatives needed to modernize the financial system while ensuring its stability and resilience in the face of emerging technological and cybersecurity challenges.

Kaur et al., (2021) conducted a comprehensive exploration of cybersecurity management in the context of financial technology (Fintech). The main objective of their research was to provide readers with a deep understanding of cybersecurity principles and practices within the Fintech industry. The authors began by introducing the fundamentals of both Fintech and cybersecurity, highlighting the critical importance of cybersecurity for financial institutions. They illustrated the significance of cybersecurity through real-world examples of cyber breaches, attacks, and resulting financial losses. Subsequently, the book delved into the intricate landscape of cyber threats, identifying potential adversaries and the vulnerabilities they exploit within Fintech systems. Moreover, the authors addressed the essential aspects of cybersecurity threat, vulnerability, and risk management specific to the Fintech sector. They presented various threat modeling strategies, focusing on attackers, assets, and software, while also discussing the

challenges associated with managing cyber risks in Fintech. Furthermore, the book offered detailed insights into cybersecurity policies and strategies tailored for securing financial institutions, accompanied by recommendations to safeguard against cyber-attacks. Overall, the study aimed to equip readers with the knowledge and tools necessary to navigate the complex cybersecurity landscape within the rapidly evolving Fintech industry.

Chen et al., (2021) conducted a study aimed at investigating the impact of Fintech products (FTPs) on the performance of commercial banks in China amidst the backdrop of the COVID-19 pandemic. Utilizing a quantitative approach, the researchers distributed self-designed questionnaires to both customers and employees of commercial banks in China. The study employed structural equation modeling to analyze the collected data. The findings of the study revealed that perceived usefulness (PU) of FTPs had a positive and significant impact on customer satisfaction, as well as on the low expectation of bank employee assistance, service quality, and work efficiency. Conversely, perceived difficulty of use (PD) of FTPs had a negative and significant impact on customer satisfaction and low expectation of assistance from bank employees. Interestingly, a positive and significant relationship was observed between PD and banks' service quality and work efficiency, indicating that these factors could mitigate some of the challenges associated with using FTPs. Overall, the study shed light on the need to enhance understanding of the effects of FTPs on non-financial firm performance, providing valuable insights for commercial banks in China by considering both customer and employee perspectives.

Hassan et al., (2021) conducted a comprehensive review focusing on cybersecurity practices within the global banking sector, with a specific emphasis on Nigerian banking institutions. Employing a qualitative research approach, the study aimed to provide an in-depth analysis of cybersecurity measures adopted by Nigerian banks amidst the backdrop of escalating cyber threats worldwide. The researchers explored various facets of cybersecurity, including regulatory frameworks, incident response mechanisms, and collaborative efforts with international cybersecurity entities. Through case studies and real-world examples, the study elucidated the evolving landscape of cyber risks faced by both global and Nigerian banks. Additionally, the effectiveness of cybersecurity measures implemented by Nigerian banks was assessed, highlighting the nation's response to these evolving threats. The study also delved into collaborative initiatives aimed at enhancing

information sharing, threat intelligence, and collective defense mechanisms among Nigerian banks and regulatory bodies. Furthermore, the role of public awareness campaigns in fostering a cyber-resilient banking environment was explored. Overall, the findings underscored the importance of ongoing adaptation, collaboration, and innovation in safeguarding the integrity and trustworthiness of banking systems globally, with specific insights provided into Nigerian banking practices.

Najaf et al., (2021) delved into the intricate relationship between Fintech firms and banks, focusing on the critical aspect of cybersecurity risk and its implications for sustainability. Employing a qualitative research approach, the study aimed to elucidate the challenges posed by the collaboration between banks and Fintech organizations in the context of cybersecurity. The researchers argued that while the alliance between banks and Fintech firms offers potential benefits in terms of profitability and sustainability, it also brings about significant cybersecurity risks. Through the development of a theoretical model, the study identified various types of cybersecurity risks inherent in such collaborations. By examining the dynamics of the banking and Fintech sectors, the researchers underscored the need for a pragmatic approach in navigating this dilemma. They emphasized the importance of collaborative efforts between banks and Fintech firms to mitigate cybersecurity risks effectively. The study concluded that while the collaboration between banks and Fintech firms holds promise for enhancing profitability and meeting market demands, addressing cybersecurity concerns is paramount for ensuring long-term sustainability. Overall, the findings shed light on the complex interplay between financial institutions and Fintech firms in the digitalized landscape, emphasizing the critical role of cybersecurity in shaping the future trajectory of banking sustainability.

Ebrahim et al., (2021) undertook a thorough examination of the opportunities and challenges presented by the integration of Fintech within the banking sector. Their study aimed to furnish a holistic portrayal of the novel prospects engendered by Fintech adoption in banking, alongside delineating the potential risks and hurdles inherent in its assimilation. Employing a qualitative research approach, the authors synthesized a comprehensive overview of the transformative impact of Fintech, emphasizing its capacity to enhance digital banking experiences, deliver personalized customer services, fortify data security measures, and offer cost-effective and efficient financial services. Conversely, the study underscored the manifold risks attendant to Fintech implementation, encompassing security, technical, regulatory, financial, and reputational

dimensions. Furthermore, the authors identified and expounded upon the plausible challenges associated with Fintech adoption, spanning technological adaptation, risk mitigation strategies, regulatory compliance, and human capital utilization.

Thach et al., (2021) investigated the impact of Industry 4.0 and digital technology on banking activities in emerging markets, with a focus on Vietnam. The study aimed to address the increasing importance of technology quality management and cybersecurity risk management in the banking sector, particularly in a rapidly growing economy like Vietnam. Utilizing a case study approach, the researchers analyzed the main technologies driving the Industry 4.0 revolution, including Big Data database technologies, Cloud Computing, Machine Learning, IoT, AI, Business Intelligence, Data Mining, and Blockchain Technologies. These technologies have been progressively integrated into banking operations and enhanced security procedures, highlighting the critical role of IT and cybersecurity risk management. Additionally, the study emphasized the sudden changes in the operating environment, such as those triggered by the COVID-19 pandemic, which have necessitated expanded remote operations in the financial sector and increased vulnerabilities to cybersecurity threats. As a result, organizations are urged to invest in new ICT and cybersecurity measures to effectively adapt to unforeseen circumstances and ensure better quality management of technology. The findings underscore the importance of proactive measures in addressing cybersecurity risks and leveraging technology advancements for sustainable development in the banking industry.

Stanikzai and Shah (2021) conducted an evaluation of cyber security threats in banking systems, aiming to assess the effectiveness of existing cyber security methods in mitigating financial crime and achieving the CIA (Confidentiality, Integrity, and Availability) business model. The study was motivated by the vulnerability of financial institutions, including banks, to cyber-attacks, which pose significant risks such as extortion, robbery, and fraud. With approximately 1.2 billion adults having bank accounts globally, the researchers recognized the critical need to enhance cyber security measures to safeguard financial systems. The research design likely involved a comprehensive literature review to identify prevalent cyber security threats in banking systems, followed by an analysis of recommended solutions and methodologies to address these threats. The study might have utilized quantitative or qualitative methods to assess the effectiveness of existing cyber security methods and propose security recommendations for potential improvements. The findings of the research contribute to understanding the evolving

landscape of cyber security threats in the financial sector and offer insights into enhancing security measures to combat financial crime effectively.

Kondratyeva et al., (2021) explored the role of information technologies in ensuring banking security, aiming to justify the importance of innovative technologies in maintaining the necessary level of security and improving the protection and resilience of domestic banking systems against external threats. The research utilized general scientific methods such as analysis and synthesis, generalization, interpretation of graphic information, and statistical analysis. Through practical examples, the authors discussed the possibilities of innovative technologies in banking and advocated for the implementation of modern security systems to create a safe business space for banks. The study delved into the main trends and leading technologies in information security, emphasizing the importance of tracking threats and risks associated with user information and resources in a fast and timely manner. Various modern information technologies and methods, including Paperless Office technology, deactualization risks, social engineering, biometric identification, psychology of information security, and regulatory and supervisory technologies, were examined. The findings revealed that while the development of innovative financial technologies and digitalization of business processes in banking offer opportunities for improvement and modernization, they also pose challenges due to the potential misuse of advanced technologies by scammers. Overall, the study highlighted the dual nature of advanced technologies in banking, characterized by both merits and downsides, and underscored the need for a balanced approach to leveraging technology for enhancing banking security.

Jayalath and Premaratne (2021) conducted an analysis focusing on the key digital technology infrastructure and cybersecurity factors pertinent to Fintech companies. The study aimed to explore how Fintech companies have revolutionized the financial industry through the adoption of emerging technologies such as Artificial Intelligence, Robotic Process Automation, and Natural Language Processing, among others. By leveraging these technologies and enhancing digital literacy among customers, Fintech companies have significantly improved customer service by providing convenient and accessible financial solutions. However, as the digital disruption caused by Fintech initiatives continues to unfold, established financial institutions like banks have also embraced Fintech to cater to the evolving needs of customers. Consequently, there has been a proliferation of digital financial platforms, leading to increased cyber threats. Therefore,

the study underscored the critical importance for Fintech companies, banks, and financial institutions to establish robust digital technology infrastructure prioritizing resilience, performance, and security. Through their analysis, Jayalath and Premaratne highlighted the imperative for Fintech companies to adapt to the highly competitive digital financial landscape by implementing structured digital technology infrastructure capable of withstanding cyber threats and ensuring the seamless delivery of financial services.

Al-Duhaidahawi et al., (2020) conducted a study to analyze the effects of Fintech variables on cybersecurity in Iraqi banks. The main objective of their research was to investigate the impact of various Fintech variables on cybersecurity, with a focus on identifying correlations and influence factors. Utilizing a quantitative research design, the authors developed hypotheses based on statistical analysis of research variables. Their findings revealed a positive relationship between Fintech variables and cybersecurity, with all correlation coefficients indicating significance at the zero point zero one level. Moreover, the influence factor analysis demonstrated a positive effect of financial technology on cybersecurity, with a significant increase in the influence coefficient to zero point nine zero eight. This suggests complementarity between different sections of the independent variable, highlighting the interconnectedness and importance of Fintech in enhancing cybersecurity measures in Iraqi banks. The study contributes to the understanding of the evolving relationship between financial technology and cybersecurity, providing insights into the factors influencing cybersecurity resilience in the banking sector.

Al-Alawi and Al-Bassam (2020) conducted a study to explore the significance of cybersecurity systems in managing risk within the banking and financial sector. The main objective of their research was to demonstrate the benefits of implementing cybersecurity measures in organizations, particularly in the banking sector, and to encourage their adoption for information security and risk management purposes. The researchers utilized an online questionnaire distributed to 100 bankers in 26 banks, with responses obtained from 35 participants representing conventional banks, Islamic banks, insurance companies, investment banks, and capital markets. The findings revealed that financial institutions in Bahrain face various cybersecurity risks, including online identity theft, deliberate system damage, and hacking, with a significant percentage reporting frequent cyber-attacks. The study also highlighted the role of the board of directors and executive managers in addressing cyber threats, emphasizing the importance of security policies,

adequate funding, and security awareness training. Additionally, the research identified a significant skills gap among employees, particularly in technical skills and communication, which poses challenges in responding to cyber-attacks effectively. The study provides valuable insights into the current cybersecurity landscape in the banking and financial sector, offering recommendations for enhancing cybersecurity measures and addressing skill deficiencies to mitigate cyber risks effectively.

Smith and Dhillon (2020) aimed to explore the potential of blockchain technology in improving the cybersecurity of financial transactions, addressing the challenge of assessing this potential solution. The study employed Keeney's (1992) multi-objective decision analytics technique, known as value-focused thinking (VFT), to evaluate the strategic values of organizations and assess the effectiveness of blockchain implementation for financial cybersecurity. The research pursued three key objectives: firstly, identifying important objectives based on organizational strategic values for evaluating cybersecurity in financial transactions; secondly, determining how these objectives can be utilized to ensure cybersecurity within financial organizations; and thirdly, evaluating blockchain as a potential solution for enhancing cybersecurity relative to existing methods. Through the application of VFT, the study demonstrated the viability of this technique as a multi-criteria decision analysis tool for assessing blockchain technology. The findings underscored the potential value of blockchain in enhancing cybersecurity in financial transactions and provided insights into how organizations can utilize VFT to assess the suitability of blockchain implementation based on their strategic objectives. Moreover, the study outlined a clear framework for extending and adapting the VFT model for individual organizational use, thereby offering practical guidance for organizations seeking to leverage blockchain for cybersecurity enhancement in the financial sector.

Demirkan et al. (2020) investigated the current and potential applications of blockchain technology in business, focusing specifically on its roles in accounting and cybersecurity. Utilizing a literature review approach, the study examined various topics including Big Data in Accounting, blockchain's implications for financial security and cybersecurity, and its utilization in financial accounting through ledger technology. Additionally, the research delved into the Department of Homeland Security's cybersecurity plans to comprehend the future trajectory of cybersecurity development. The findings revealed that blockchain has significant implications for auditing practices, potentially leading to

drastic changes in the profession. Moreover, the study emphasized the importance of effectively integrating blockchain into different facets of cybersecurity and accounting, particularly in auditing and general accounting procedures. The research aimed to shed light on the transformative potential of blockchain technology in enhancing security and efficiency within business processes, especially in the realms of accounting and cybersecurity. Through a comprehensive review of existing literature and government plans, the study provided insights into the evolving landscape of cybersecurity and accounting practices, highlighting the need for proactive adoption of blockchain to address emerging challenges and opportunities in these domains.

Uddin et al., (2020) conducted a systematic review to examine the pervasive effects of cybersecurity risk on the financial system, aiming to synthesize existing literature and identify avenues for future research. Through a comprehensive analysis of conceptual discussions, technical analyses, survey results, and policy documents, the study highlighted the significant threat posed by cybersecurity risk to the financial sector. While acknowledging the abundance of literature on the subject, the researchers noted a scarcity of empirical studies based on real data, indicating a gap in current research efforts. The synthesis focused on dimensions detrimental to banking system vulnerability, shedding light on the multifaceted nature of cybersecurity challenges faced by financial institutions. Additionally, the study reviewed guidelines suggested by international and national regulatory bodies to assist banks and financial institutions in managing cyber risk exposure. In conclusion, the researchers proposed five new research avenues aimed at enhancing understanding of cybersecurity risk and aiding practitioners in developing robust cyber risk management frameworks. By addressing these research avenues, future studies have the potential to contribute significantly to the knowledge base on cybersecurity risk in the financial sector and improve risk management practices.

Didenko (2020) conducted an insightful analysis of cybersecurity regulation in Singapore's financial sector, particularly focusing on its implications for domestic Fintech firms. The researcher identified cybersecurity as a top priority for Singapore's regulators in their pursuit of establishing a Smart Financial Centre. Through an examination of bespoke cybersecurity rules developed by Singaporean regulators, Didenko shed light on the challenges faced by smaller and less sophisticated players, such as Fintech innovators, in implementing cybersecurity measures effectively. The paper highlighted the increasing complexity and interconnectedness of the financial services ecosystem, which amplifies

the risks of cyber-attacks and contagion. Didenko argued that while Singapore is well-positioned to lead by example in the Asia-Pacific region by developing and implementing innovative regulatory approaches to cybersecurity, true international harmonization in this area remains a distant possibility. The study underscores the importance of tailored regulatory measures to ensure the cybersecurity of smaller entities within the financial sector, given their limited resources and expertise compared to larger institutions. Overall, Didenko's research contributes valuable insights into the evolving landscape of cybersecurity regulation and its implications for the Fintech sector, both domestically and internationally.

Adeyoju (2019) delved into the critical challenges posed by cybercrime and cybersecurity within the realm of financial technology (Fintech). Through a qualitative analysis, the study aimed to elucidate the profound impact of cyber threats on Fintech companies, particularly startups, and explore the measures employed to safeguard their data and infrastructure. Tracing the evolution of Fintech from regulatory changes post the Great Depression to its exponential growth following the global financial crisis of 2008, the researcher highlighted the transformative role of Fintech in revolutionizing various aspects of banking and financial services. However, the study underscored the inherent vulnerabilities of Fintech companies to cybercriminal activities due to the nature of their operations, which encompass a wide range of financial activities susceptible to exploitation. By examining the dynamics of cybercrime in the context of Fintech, the study shed light on the strategies adopted by these companies to mitigate cybersecurity risks and protect their assets. The findings emphasized the need for robust cybersecurity measures and proactive risk management practices to safeguard the integrity and security of Fintech operations. Overall, the study provided valuable insights into the complex interplay between cyber threats and the Fintech landscape, highlighting the imperative for continuous innovation and vigilance in addressing cybersecurity challenges within the industry.

Nuyens (2019) conducted an investigation into the disruptive impact of Fintech and digital technologies on banks and regulators. The study aimed to elucidate the extent to which these technological advancements have reshaped the landscape of banking and regulatory practices. Employing a qualitative research approach, the author delved into the evolving dynamics of the banking sector in response to technological innovations, emphasizing banks' endeavors to leverage new technologies for enhanced product

delivery and customer experience. The study identified both risks and opportunities arising from technological change, noting that while advancements such as Fintech partnerships have introduced new avenues for growth and efficiency, they have also heightened the prevalence of risks such as cyberattacks and money laundering. Moreover, the study highlighted the evolving role of regulators and supervisors in adapting to the Fintech ecosystem, gradually incorporating technological advancements into their oversight frameworks to ensure the stability and integrity of financial markets. Ultimately, this study underscored the transformative potential of Fintech and digital technologies in fostering a more interconnected and competitive landscape, wherein banks, tech companies, regulators, and supervisors collaborate to deliver improved financial services and societal value. However, the author emphasized the importance of ensuring a level playing field to mitigate potential disparities and safeguard the interests of all stakeholders involved.

Buckley et al., (2019) conducted a comprehensive analysis of the evolving landscape of financial technology (Fintech) and its associated risks. Their primary objective was to examine the intersection of digitization, datafication, and emerging technologies such as cloud computing, blockchain, big data, and artificial intelligence within the realm of finance. Through a thorough examination of developments in both developed and emerging markets, the researchers highlighted the emergence of cybersecurity and technological risks as significant threats to financial stability and national security. Furthermore, they discussed the entry of major technology firms, termed TechFins, into the financial sector, which brings forth new challenges related to potentially systemically important infrastructure and the concentration of data. The authors emphasized the potential for systemic risk arising from phenomena such as "Too Big to Fail" and "Too Connected to Fail" in the context of data-driven financial activities. In conclusion, they proposed basic principles for monitoring and addressing these risks, with a particular focus on the role of regulatory technology (RegTech). This study provides valuable insights into the complex dynamics of Fintech and underscores the importance of proactive risk management strategies in the face of rapid technological advancements in the financial industry.

Callen-Naviglia and James (2018) conducted a literature review to explore the significance of cybersecurity in the context of Fintech and RegTech. With the rise of consumer demand for remote banking services and e-commerce convenience, financial

institutions are compelled to embrace technological advancements, leading to the emergence of Fintech. However, the regulatory landscape has also evolved with the proliferation of Fintech, giving rise to RegTech aimed at overseeing these innovative products and services. Amidst these developments, cybersecurity emerges as a critical factor influencing the success and ongoing progress of both Fintech and RegTech. The study aimed to address several key questions: whether advancing Fintech impedes regulators' roles, if RegTech can adequately adapt to the evolving demands of Fintech, and whether cybersecurity measures are sufficiently robust to protect against financial threats. Through their literature review, Callen-Naviglia and James sought to shed light on the interplay between Fintech, RegTech, and cybersecurity, aiming to provide insights into the challenges and opportunities presented by the integration of technology in the financial sector. Their findings contribute to the understanding of the complex dynamics between technological innovation, regulatory oversight, and cybersecurity, highlighting the need for effective cybersecurity measures to ensure the resilience of financial systems in the digital age.

Ng and Kwok (2017) conducted a study focusing on the strategic approach adopted by the regulator of a global financial center (GFC) in response to the emergence of financial technology (Fintech) and cybersecurity challenges. The main objective was to explore how the regulator articulates opportunities and risks associated with Fintech within the context of Hong Kong as a GFC. The research employed a literature review to examine the global regulatory environment and the risks posed by Fintech, particularly cybersecurity. By analyzing policy documents disclosed by the financial regulator, the study investigated the formulation and implementation of regulatory policies aimed at addressing cybersecurity concerns. The findings revealed that the financial regulator adopted a strategic approach that embraced the opportunities presented by Fintech while implementing comprehensive risk-based mechanisms to manage cyber risks effectively. Strategic controls were employed to promote cybersecurity institutionalization among regulated firms. The study also proposed a pathway for developing a profession equipped with both technical and ethical competencies to mitigate emerging risks associated with Fintech. However, the effectiveness of this approach in addressing fraud exposures arising from rapid Fintech developments across borders remains untested. Overall, the research shed light on the strategic response of regulators to the evolving landscape of

Fintech and cybersecurity in GFCs, providing insights into regulatory policies and their implications for financial institutions.

Vasiljeva and Lukanova (2016) embarked on a comprehensive exploration of the evolving dynamics between commercial banks and Fintech companies within the landscape of digital transformation in the financial industry. Their study aimed to scrutinize, assess, and juxtapose the interplay between these two entities while discerning the developmental trajectory of commercial banking amid the burgeoning influence of Fintech companies. Utilizing a mixed-methods approach, the researchers employed a combination of literature review, secondary data analysis, and primary data collection through surveys and interviews. The analysis encompassed an evaluation of financial parameters of Fintech firms, including investments from international banks, to glean insights into their impact on traditional banking models. Central to their investigation was the probing question of whether non-banking entities could pose a formidable challenge to traditional banking practices to the extent of usurping their established domains. The study unfolded against the backdrop of transformative technological innovations reshaping consumer behaviors and perceptions of financial services, propelling banking into a realm where physical branches give way to digital interfaces.

Table 1

Empirical Review Summary Table

S.N.	Researcher/s	Title	Objective	Methodology	Findings
1	Samoei and Gatobu (2024)	Cybersecurity and Performance of Internet Banking Services in Commercial Banks in Nairobi City County, Kenya	To assess the impact of cybersecurity on the performance of internet banking services in commercial banks within Nairobi City County, Kenya	Descriptive research design; structured questionnaire	Application security significantly influences the performance of internet banking services; IT governance is crucial for enhancing trust, customer satisfaction, and competitiveness
2	Umoga et al., (2024)	Critical Review of Emerging Cybersecurity Threats in Financial Technologies	To analyze the challenges and vulnerabilities faced by financial institutions amidst the rapid evolution of financial	Descriptive Research Design	Cyber threats range from traditional phishing to sophisticated ransomware; regulatory frameworks and human factors play significant roles in

S.N.	Researcher/s	Title	Objective	Methodology	Findings
			technologies		mitigating risks
3	Alsakini et al., (2024)	Impact of Cybersecurity Breaches on the Quality of Financial Accounting Statements in Selected Banks in Jordan	To investigate the impact of cybersecurity breaches on the quality of financial accounting statements in selected banks in Jordan	Utilized primary and secondary data; structured questionnaires	Cybersecurity breaches significantly impact the quality of financial accounting statements, with specific types of breaches showing varying effects on different aspects of financial statements
4	Farayola (2024)	Revolutionizing Banking Security: Integrating AI, Blockchain, and Business Intelligence for Enhanced Cybersecurity	To propose a methodology integrating AI, Blockchain, and BI to revolutionize banking security	Conceptual framework development	Integration of AI, Blockchain, and BI can enhance banking security by enabling proactive defense mechanisms, secure transactions, and actionable insights
5	Choithani et al., (2024)	Comprehensive Study of AI and Cybersecurity on Bitcoin, Cryptocurrency, and Banking System	To conduct a comprehensive study on the role of AI and cybersecurity in Bitcoin, cryptocurrency, and the banking system	Descriptive Research Design	AI techniques can play a significant role in addressing various aspects related to cryptocurrencies, including risk reduction, price prediction, and fraud detection
6	Gholami et al., (2023)	Factors Influencing the Integration of Fintech in Iran's Banking Sector: A Descriptive-Analytical Study	To explore factors influencing the integration of Fintech within Iran's banking sector	Descriptive-analytical research design; questionnaire	Legal frameworks and infrastructure enhancement are crucial for facilitating Fintech integration in Iran's banking sector
7	Dung et al., (2023)	Financial Technology in Commercial Banks: Situation and Solutions	To explore the application of financial technology in commercial banks and propose solutions to	Descriptive Research Design; potentially surveys or interviews	Fintech applications have transformed various facets of commercial banking, reshaping market structures and long-term development plans

S.N.	Researcher/s	Title	Objective	Methodology	Findings
			enhance its efficiency		
8	Despotovic et al., (2023)	Cybercrime and Cybersecurity in Financial Technologies: An Analysis	To analyze cyber threats and vulnerabilities in financial technologies and propose solutions to mitigate risks	Descriptive Research Design; systematic analysis	User awareness and employee training are crucial in mitigating cyber threats; proactive cybersecurity measures are necessary to safeguard financial systems
9	Akintoye et al., (2022)	Cybersecurity and Financial Innovation of Selected Deposit Money Banks in Nigeria	To assess the impact of cybersecurity on the financial innovation of selected Deposit Money Banks (DMBs) in Nigeria	Survey research design; structured questionnaires	Cybersecurity has a statistically significant positive impact on the financial innovation of DMBs in Nigeria
10	Scheau et al., (2022)	Key Pillars for Fintech and Cybersecurity	To address the need for responsible cybersecurity policies and regulations in the context of the rapid digitalization of financial services	Descriptive Research Design	Proactive cybersecurity measures are essential in mitigating cyber risks effectively in the financial services sector
11	Vucinic and Luburic (2022)	Intersection of Fintech, Risk-Based Thinking, and Cyber Risk in Modernizing the Financial System	To examine developments in Fintech, its benefits, risks, and the role of monetary authorities in managing changes while preserving stability	Qualitative research; Fintech SWOT analysis	Artificial intelligence drives Fintech development; Risk-based thinking crucial in navigating Fintech opportunities and threats; Cyber risk identified as a significant threat in Fintech landscape

S.N.	Researcher/s	Title	Objective	Methodology	Findings
12	Kaur et al., (2021)	Cybersecurity Management in Financial Technology: Principles and Practices	To provide a deep understanding of cybersecurity principles and practices within the Fintech industry	Descriptive Research Design	Cybersecurity crucial for financial institutions; Various cyber threats and vulnerabilities in Fintech systems; Strategies for cybersecurity threat, vulnerability, and risk management
13	Chen et al., (2021)	Impact of Fintech Products on the Performance of Commercial Banks in China Amidst COVID-19	To investigate the impact of Fintech products on the performance of commercial banks in China	Quantitative approach; Structural equation modeling	Perceived usefulness of FTPs positively impacts customer satisfaction; Perceived difficulty of use negatively impacts customer satisfaction; Challenges associated with using FTPs can be mitigated by service quality and work efficiency
14	Hassan et al., (2021)	Cybersecurity Practices in Global Banking: A Focus on Nigerian Banking Institutions	To analyze cybersecurity measures adopted by Nigerian banks and their effectiveness	Qualitative research; Case studies	Nigerian banks respond to evolving cyber threats; Collaborative efforts enhance cybersecurity measures; Public awareness campaigns foster a cyber-resilient banking environment
15	Najaf et al., (2021)	Cybersecurity Risks in Banking-Fintech Collaborations: Implications for Sustainability	To explore cybersecurity risks in banking-Fintech collaborations and their implications for sustainability	Qualitative research; Theoretical model development	Collaboration between banks and Fintech firms poses cybersecurity risks; Collaborative efforts essential for mitigating cybersecurity risks and ensuring sustainability
16	Ebrahim et al., (2021)	Opportunities and Challenges of Fintech Integration in the Banking Sector	To provide an overview of opportunities and challenges of Fintech integration in the	Qualitative research; Descriptive Research Design	Fintech enhances digital banking experiences but poses security, technical, regulatory,

S.N.	Researcher/s	Title	Objective	Methodology	Findings
			banking sector		financial, and reputational challenges; Strategies for addressing challenges
17	Thach et al., (2021)	Industry 4.0, Digital Technology, and Banking Activities in Emerging Markets: A Focus on Vietnam	To investigate the impact of Industry 4.0 and digital technology on banking activities in emerging markets	Case study approach	Industry 4.0 technologies integrated into banking operations; Importance of IT and cybersecurity risk management highlighted
18	Stanikzai and Shah (2021)	Evaluation of Cybersecurity Threats in Banking Systems	To assess the effectiveness of existing cybersecurity methods in mitigating financial crime in banking systems	Descriptive Research Design; Potentially quantitative or qualitative analysis	Vulnerability of financial institutions to cyber-attacks; Effectiveness of existing cybersecurity methods examined
19	Kondratyeva et al., (2021)	Role of Information Technologies in Ensuring Banking Security	To justify the importance of innovative technologies in maintaining banking security	General scientific methods	Innovative technologies offer opportunities but pose challenges; Importance of tracking threats and risks associated with user information and resources
20	Jayalath and Premaratne (2021)	Analysis of Digital Technology Infrastructure and Cybersecurity Factors in Fintech Companies	To explore the digital technology infrastructure and cybersecurity factors in Fintech companies	Descriptive Research Design; Analysis	Fintech companies revolutionize financial industry through emerging technologies; Importance of robust digital technology infrastructure and cybersecurity emphasized
21	Al-Duhaidahawi et al., (2020)	Effects of Fintech Variables on Cybersecurity in Iraqi Banks	To analyze the impact of Fintech variables on cybersecurity in Iraqi banks	Quantitative research; Statistical analysis	Positive relationship between Fintech variables and cybersecurity; Complementarity between different sections of Fintech variables observed

S.N.	Researcher/s	Title	Objective	Methodology	Findings
22	Al-Alawi and Al-Bassam (2020)	Significance of Cybersecurity Systems in Managing Risk in the Banking and Financial Sector	To demonstrate the benefits of implementing cybersecurity measures in organizations, particularly in the banking sector	Online questionnaire ; Qualitative analysis	Financial institutions in Bahrain face various cybersecurity risks; Role of board of directors and executive managers emphasized
23	Smith and Dhillon (2020)	Potential of Blockchain Technology in Improving Financial Transaction Cybersecurity	To explore the potential of blockchain technology in enhancing the cybersecurity of financial transactions	Keeney's multi-objective decision analytics technique (Value-focused thinking)	Blockchain has potential to enhance cybersecurity in financial transactions; Value-focused thinking viable for assessing blockchain implementation
24	Demirkan et al., (2020)	Applications of Blockchain Technology in Business: Focus on Accounting and Cybersecurity	To investigate current and potential applications of blockchain technology in business, with emphasis on accounting and cybersecurity	Descriptive Research Design	Blockchain has implications for auditing practices; Importance of integrating blockchain into cybersecurity and accounting highlighted
25	Uddin et al., (2020)	Pervasive Effects of Cybersecurity Risk on the Financial System: A Systematic Review	To examine the effects of cybersecurity risk on the financial system and identify avenues for future research	Systematic review	Significant threat posed by cybersecurity risk to financial sector identified; Five research avenues proposed for future studies
26	Didenko (2020)	Cybersecurity Regulation in Singapore's Financial Sector: Implications for Domestic Fintech Firms	To analyze cybersecurity regulation in Singapore's financial sector and its implications for domestic Fintech firms	Qualitative analysis; Examination of regulations	Singapore prioritizes cybersecurity in financial regulation; Challenges faced by smaller Fintech firms highlighted
27	Adeyoju (2019)	Impact of Cyber Threats on Financial Technology (Fintech) Companies	To explore the impact of cyber threats on Fintech companies and examine measures to safeguard data	Qualitative analysis	Fintech vulnerable to cybercriminal activities; Importance of robust cybersecurity measures emphasized

S.N.	Researcher/s	Title	Objective	Methodology	Findings
			and infrastructure		
28	Nuyens (2019)	Disruptive Impact of Fintech and Digital Technologies on Banks and Regulators	To elucidate the impact of Fintech and digital technologies on banks and regulators	Qualitative research	Technological advancements reshape banking sector; Risks and opportunities identified
29	Buckley et al., (2019)	Evolution of Financial Technology (Fintech) and Associated Risks	To analyze the evolution of Fintech and associated risks, focusing on digitization and emerging technologies	Descriptive Research Design; Analysis	Cybersecurity and technological risks pose threats to financial stability; Role of regulatory technology (RegTech) emphasized
30	Callen-Naviglia and James (2018)	Significance of Cybersecurity in the Context of Fintech and RegTech	To explore the significance of cybersecurity in the context of Fintech and RegTech	Descriptive Research Design	Cybersecurity is critical for the success of Fintech and RegTech; Effective cybersecurity measures needed to protect financial systems in the digital age
31	Ng and Kwok (2017)	Strategic Response of a Global Financial Center Regulator to Fintech and Cybersecurity Challenges	To investigate the strategic response of a financial center regulator to Fintech and cybersecurity challenges	Descriptive Research Design; Analysis of policy documents	Regulator adopts strategic approach embracing Fintech opportunities while managing cyber risks effectively; Proposal for developing a profession equipped to mitigate Fintech-related risks
32	Vasiljeva and Lukanova (2016)	Dynamics between Commercial Banks and Fintech Companies in the Digital Transformation of the Financial Industry	To explore the evolving dynamics between commercial banks and Fintech companies in the context of digital transformation	Mixed-methods approach; Descriptive Research Design, secondary data analysis, surveys, interviews	Fintech firms impact traditional banking models; Technological innovations reshape consumer behaviors and perceptions of financial services; Digital interfaces replace physical branches

2.4 Research Gap

In prior research conducted by Callen-Naviglia and James (2018), Ng and Kwok (2017), and Vasiljeva and Lukanova (2016), the significance of cybersecurity within the context of financial technology (Fintech) has been explored. These studies have highlighted the importance of effective cybersecurity measures in ensuring the success and resilience of Fintech initiatives, particularly in global financial centers. However, a notable gap exists in research specific to the Nepalese commercial banking industry. Despite extensive investigations in various contexts, including developed economies and emerging markets, such as those conducted by Adeyoju (2019), Nuyens (2019), and Buckley et al. (2019), there remains a lack of focused inquiry into the dynamics of Fintech and cybersecurity within the Nepalese banking landscape. Therefore, further research is warranted to address this context gap and provide insights into the analysis of impact of finetech on cybersecurity in commercial banks in Nepal.

Furthermore, there exists a time gap in the literature. Many existing studies have utilized data from previous years, potentially limiting the relevance and applicability of their findings to the current landscape. In contrast, the study in question utilizes data from 2024, providing a more up-to-date understanding of the Fintech and cybersecurity landscape in Nepal's commercial banks.

Moreover, there is a variable gap observed across the reviewed studies. While several studies have examined various factors influencing cybersecurity, such as organizational culture, security policies, and technological infrastructure, not all have included key variables like self-efficacy, information security awareness, technological culture, and competence and skill as components of Fintech affecting cybersecurity resilience. This omission highlights the need for a more comprehensive examination of the multifaceted nature of Fintech and its implications for cybersecurity.

Lastly, there is a methodology gap present in the literature. While many studies have employed quantitative or qualitative research methods, such as surveys, interviews, or case studies, few have utilized a descriptive statistics approach combined with a causal comparative research design. This gap suggests a research to employ innovative methodological approaches to better understand the complex relationships between Fintech implementation and cybersecurity outcomes.

Overall, the identified research gaps underscore the need for further investigation into the specific context of Fintech and cybersecurity within Nepal's commercial banking sector, utilizing up-to-date data, incorporating comprehensive variables, and employing innovative research methodologies. The study in question aims to address these identified gaps by providing a detailed examination of Fintech and cybersecurity in Nepalese commercial banks, thereby contributing to the existing body of knowledge in this field.

CHAPTER III
RESEARCH METHODOLOGY

This chapter details the research methodology employed in the study. The research design outlines the overall strategy and approach used to address the research questions. Population and sample, and sampling design discusses the target population, sample size, and the techniques used for selecting participants. The nature and sources of data and the instrument of data collection section describes the types of data utilized, their origins, and the tools and procedures for data collection. The method of analysis explains the techniques and processes applied to analyze the gathered data. Lastly, the research framework and definition of variables provides a conceptual model of the study and defines the key variables involved.

3.1 Research Design

This study has adopted both a descriptive research design and a causal comparative research design. Descriptive statistics have been utilized to assess the current status of cybersecurity, while causal comparative research design has been employed to analyze the impact of financial technology on cybersecurity.

3.2 Population and Sample, and Sampling Design

This study has focused on financial technology and cybersecurity in commercial banks in the Kathmandu Valley, Nepal. The total population comprises all employees working in commercial banks located at Kathmandu Valley. A sample size of 385 employees has been chosen using convenience sampling for ease of data collection in accordance with the study's requirements. The data has been collected from employee of various commercial banks in Nepal as follows.

Given that the target population for this study is very large and unknown, Cochran developed an equation to determine a representative sample size for proportions. The formula is:

$$n_0 = \frac{z^2 pq}{e^2}$$

Where, n_0 is Sample size, $z^2$is is the abscissa of the normal curve, p is proportion of success, q is proportion of failure(q=1-p) and $e^2$is the margin of error which is taken as 5%. Applying Cochran's formula results in a sample size of 384.16, approximately 385.

Table 2
Sample Size

S.N.	Name of Bank	Type of Bank	Sample
1	Rastriya Banijya Bank	Government Bank	55.00
2	Agriculture Development Bank	Government Bank	55.00
3	Everest Bank	Joint Venture Bank	55.00
4	NMB Bank	Joint Venture Bank	55.00
5	Nabil Bank	Joint Venture Bank	55.00
6	NIC Asia	Private Bank	55.00
7	Global IME Bank	Private Bank	55.00
	Total		385.00

3.3 Nature and Sources of Data and the Instrument of Data Collection

This study has adopted quantitative nature of data, utilizing primary sources of data collected through structured questionnaire surveys. The questionnaire design draws on insights from previous articles by Laurent & Sinz (2019), Al-Duhaidahawi et al. (2020), and Javaheri et al. (2023), as well as consultations with supervisors and senior researchers. The structured questionnaire is crafted to capture relevant variables and factors identified in the literature, ensuring alignment with existing theoretical frameworks and empirical findings. A five-point Likert scale is employed in the questionnaire, ranging from "strongly disagree" to "strongly agree," with corresponding numerical values assigned from 1 to 5. This approach enables respondents to express their opinions and perceptions regarding the variables under investigation, providing a quantitative basis for analysis and interpretation. By leveraging a structured questionnaire survey method, this study aims to gather comprehensive data that can be rigorously analyzed to address the research objectives and contribute to the existing body of knowledge in the field.

3.4 Method of Analysis

After data collection, the collected data has been presented in statistical software such as Microsoft Excel and SPSS. Subsequently, various statistical tools such as descriptive statistics, correlation analysis, and multivariate regression models have been utilized to analyze the data. Descriptive statistics have allowed for the exploration of the central tendency and dispersion of the data, providing insights into the current status of financial technology and cybersecurity in commercial banks in the Kathmandu Valley, Nepal. Additionally, correlation analysis has been employed to examine the relationships between different variables, shedding light on potential associations between financial

technology adoption and cybersecurity measures. Furthermore, multivariate regression models have been applied to investigate the impact of financial technology on cybersecurity, controlling for other relevant factors. Through these analytical approaches, the study aims to provide a comprehensive understanding of the relationship between financial technology and cybersecurity in the context of commercial banks in Nepal

3.4.1 Mean

In statistics, the mean, often referred to as the arithmetic mean or average, is a measure of central tendency that represents the typical value of a set of numbers. It is calculated by summing up all the values in a dataset and then dividing the sum by the total number of values. In this study, the mean has been used as a statistical measure to examine the current status of cybersecurity in commercial banks in Nepal. By calculating the mean of cybersecurity-related variables, such as security measures implemented, incidents of cyber threats, or level of preparedness against cyberattacks, the study aims to provide insight into the overall cybersecurity posture of commercial banks in Nepal. The mean serves as a descriptive statistic, offering a summary measure that indicates the average level or magnitude of cybersecurity within the sampled banks, helping to assess their current cybersecurity status.

$$\text{Mean} = \frac{\sum x}{n}$$

Where,

X = Value of responses of each independent or dependent variable

n = Number of responses

3.4.2 Standard Deviation (S.D.)

Standard deviation (S.D.) is a statistical measure that quantifies the amount of variation or dispersion in a set of data values. It indicates how much individual data points deviate from the mean of the dataset. A low standard deviation suggests that the data points tend to be close to the mean, while a high standard deviation indicates that the data points are spread out over a wider range of values.

In this study, standard deviation (S.D.) has been utilized to assess the variability of employees' perceptions or behaviors related to cybersecurity in commercial banks in Nepal. By calculating the standard deviation of responses to survey questions or other

relevant variables, the study aims to understand the extent to which employees' views or practices regarding cybersecurity diverge from the average. This analysis helps in gauging the level of consensus or dispersion among employees regarding cybersecurity practices within commercial banks in Nepal.

$$\text{Standard Deviation}(\sigma) = \sqrt{\frac{\sum(X - \overline{X})^2}{n}}$$

Where,

X = Value of responses of each dependent or independent variable

$\overline{X}$ = Mean value of responses of each dependent or independent variable

n= Number of responses

3.4.3 Correlation Analysis

Correlation analysis is a statistical technique used to measure the strength and direction of the relationship between two or more variables. It assesses the extent to which changes in one variable are associated with changes in another variable. The correlation coefficient, typically denoted as "r," ranges from -1 to +1. A correlation coefficient of +1 indicates a perfect positive correlation, meaning that as one variable increases, the other variable also increases proportionally. Conversely, a correlation coefficient of -1 indicates a perfect negative correlation, where one variable increases as the other decreases. A correlation coefficient of 0 suggests no linear relationship between the variables.

In this study, correlation analysis has been employed to analyze the relationship between financial technology (Fintech) and cybersecurity in commercial banks in Nepal. By calculating the correlation coefficient between these two variables, the study aims to understand the degree and direction of their association. This analysis helps in determining whether there is a significant positive or negative correlation between the adoption of financial technology and the level of cybersecurity measures implemented within commercial banks in Nepal. The correlation coefficient between two variables is also calculated by using the following formula:

$$\text{Correlation Coefficient}(r) = \frac{n\sum xy - \sum x \sum y}{\sqrt{n\sum x^2 - (\sum x)^2}\sqrt{n\sum y^2 - (\sum y)^2}}$$

Where,

n = Number of observations

x = Value of independent variable

y= Value of dependent variable

3.4.4 Regression Analysis

Regression analysis is a statistical method used to examine the relationship between one dependent variable and one or more independent variables. It helps in understanding how the independent variables influence or predict changes in the dependent variable. In multivariate regression analysis, multiple independent variables are considered simultaneously to assess their combined impact on the dependent variable.

In this study, multivariate regression analysis has been employed to analyze the impact of financial technology (Fintech) and cybersecurity on commercial banks in Nepal. By including both Fintech and cybersecurity as independent variables and assessing their effects on the dependent variable (likely a measure of bank performance or security), the study aims to uncover the extent to which these factors contribute to the overall status of commercial banks in Nepal. This analysis provides insights into how the adoption of Fintech and cybersecurity measures influences the functioning and security of commercial banks in the Nepalese context. Regression model used in this study was as follows.

$Y_{CYS} = \alpha + \beta_1 SEF + \beta_2 INS + \beta_3 TEC + \beta_4 CAS + E$ ……Eq (1)

Where,

CYS = Cyber Security

SEF = Self-Efficacy

INS = Information Security

TEC = Technological Culture

CAS = Competence and Skill

α = Intercept Term

E = Error

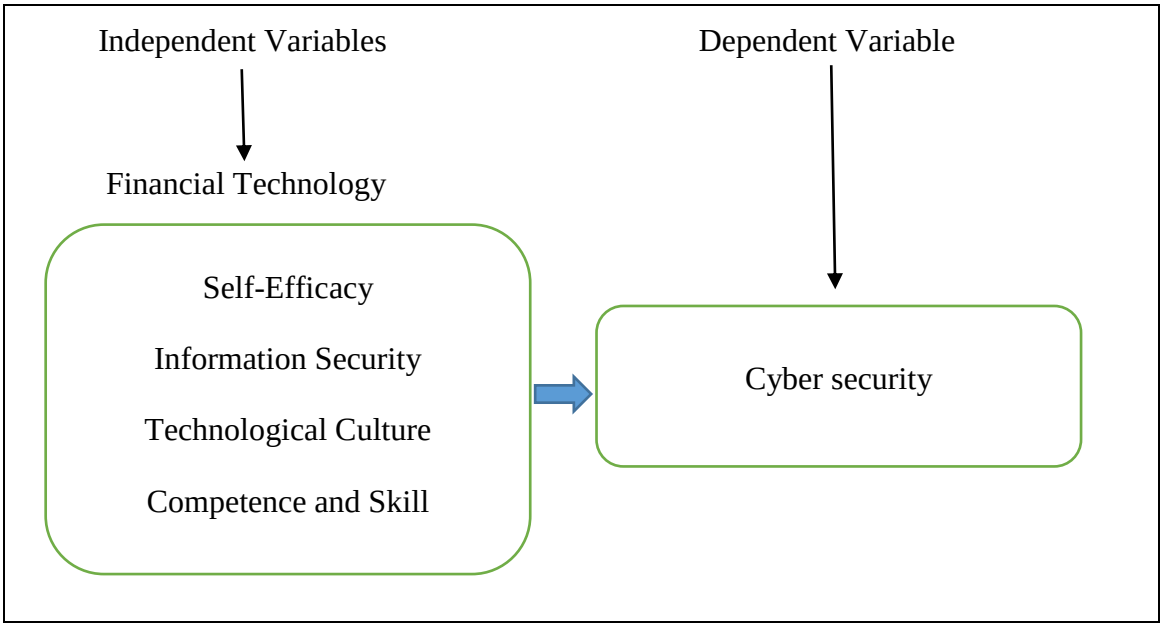
β_1, β_2, β_3, β_4= Beta Coefficients

3.5 Research Framework and Definition of Variables

3.5.1 Research Framework

A research framework serves as a conceptual structure that guides the study's investigation by organizing key concepts, variables, and relationships. It outlines the theoretical foundation upon which the research is built and provides a roadmap for data collection, analysis, and interpretation. The framework helps researchers conceptualize complex phenomena and identify the variables and factors relevant to their study.

In this study, the research framework adopted from self-efficacy, information security, technological culture, competence, and skill comprises independent variables. These variables represent individual and organizational attributes related to cybersecurity readiness and capability. The study aims to investigate how these factors influence cybersecurity in commercial banks in Nepal. Cybersecurity, the dependent variable in this framework, represents the overall security posture of commercial banks and is influenced by the various independent variables identified. By examining the relationships between self-efficacy, information security, technological culture, competence, and skill, and their impact on cybersecurity, the study seeks to provide insights into the factors shaping cybersecurity practices and resilience in the Nepalese banking sector.



Source: Al-Duhaidahawi et al. (2020)

Figure 1. Research Framework

3.5.2 Operational Definition of Variables

The operational definition of variables are as follows.

Self-Efficacy

Self-Efficacy refers to an individual's belief in their ability to perform specific tasks or achieve desired outcomes. In the context of cybersecurity, self-efficacy pertains to one's confidence in their capacity to effectively navigate and manage security challenges, such as identifying and mitigating cyber threats, adhering to security protocols, and responding to security incidents. Individuals with high levels of self-efficacy in cybersecurity are more likely to demonstrate proactive behaviors, exhibit resilience in the face of security breaches, and contribute positively to overall organizational security posture (Lee, 2021).

Information Security

Information Security encompasses the practices, policies, and measures implemented to protect sensitive information from unauthorized access, disclosure, alteration, or destruction. This includes safeguarding data confidentiality, integrity, and availability across various digital platforms and communication channels (Buckley, 2019). Effective information security measures involve implementing robust access controls, encryption techniques, intrusion detection systems, and security awareness training programs to mitigate risks posed by external threats and insider breaches.

Technological Culture

Technological Culture refers to the prevailing attitudes, beliefs, values, and norms within an organization concerning the adoption, utilization, and management of technology. A positive technological culture fosters an environment conducive to innovation, collaboration, and digital transformation (Al-Duhaidahawi et al., 2020). Organizations with a strong technological culture prioritize continuous learning, experimentation, and adaptation to emerging technologies, thereby enhancing their resilience to technological disruptions and cyber threats.

Competence and Skill

Competence and Skill encompass the knowledge, capabilities, and expertise required to effectively address cybersecurity challenges and tasks within an organization. This includes technical proficiencies in areas such as network security, cryptography, malware analysis, and incident response, as well as non-technical skills like risk management,

communication, and problem-solving (Kuzmina-Merlino & Saksonova, 2018). Competent cybersecurity professionals possess a comprehensive understanding of cybersecurity principles, best practices, and regulatory requirements, enabling them to effectively safeguard organizational assets and mitigate security risks.

Cybersecurity

Cybersecurity refers to the practice of protecting computer systems, networks, devices, and data from unauthorized access, cyberattacks, and other malicious activities. It encompasses a range of strategies, technologies, and processes designed to safeguard digital assets and ensure the confidentiality, integrity, and availability of information (Al-Duhaidahawi et al., 2020). Cybersecurity measures include implementing firewalls, antivirus software, intrusion detection systems, encryption protocols, and access controls to prevent and detect unauthorized access, as well as conducting regular security assessments and incident response planning to mitigate and address security breaches. The goal of cybersecurity is to create a secure computing environment that protects against cyber threats and supports the safe and secure use of technology for individuals, organizations, and society as a whole.

CHAPTER IV
RESULTS AND DISCUSSION

In this the findings of the study are presented, analyzed, and discussed in relation to previous research. This section systematically examines whether the results align with or diverge from established research findings. By comparing the current data with prior studies, the analysis provides a deeper understanding of the current status of cybersecurity in commercial banks in Nepal. This comparative approach helps to validate the study's results, identify trends, and highlight any unique insights or contradictions, thereby contributing to the broader discourse on cybersecurity in the banking sector.

4.1 Results

This section presents the results, including data analysis conducted using various tables. The data presentation is structured to highlight key findings and trends observed in the study. Statistical analyses are performed to interpret the collected data, providing insights into the current status of cybersecurity in commercial banks in Nepal. The tables are used to organize and illustrate the information clearly, making it easier to identify patterns and draw conclusions from the research.

4.1.1 Demographic Profile of Respondents

In section respondents provided demographic information including gender, age, educational qualifications, job positions, years of experience in the banking industry, department, and type of bank. This demographic profile offers a comprehensive overview of the participants, ensuring a diverse and representative sample for analyzing the current status of cybersecurity in commercial banks in Nepal. By capturing these details, the study aims to understand the varying perspectives and experiences of individuals across different roles and backgrounds within the banking sector.

Table 3

Demographic Profile of Respondents

Variables		Frequency	Percent
Gender	Male	207	53.80
	Female	178	46.20
Age	18-24	65	16.90
	25-34	280	72.70
	35-44	40	10.40
Educational Qualification	High School	33	8.60
	Bachelor's Degree	155	40.30
	Master's Degree	193	50.10
	Doctorate or Professional Degree	4	1.00
Job Position	Entry-level/Staff	91	23.60
	Mid-level/Manager	228	59.20
	Senior Management	66	17.10
Years of Experience in Banking Industry	0-5	181	47.00
	6-10	159	41.30
	11-15	33	8.60
	16 and above	12	3.10
Department	Operations	235	61.00
	IT/Technology	81	21.00
	Risk Management	52	13.50
	Compliance	17	4.40
Type of Bank	Private Bank	110	28.60
	Government Bank	110	28.60
	Joint Venture Bank	165	42.90

Source: Field survey, 2024

Table 3 represents the demographic profile of respondents. The demographic data indicates that 53.8% of respondents are male (n=207) and 46.2% are female (n=178). The mean score for gender perception toward financial technology and cybersecurity was analyzed, with a standard deviation that indicates a balanced representation across both genders. Respondents' ages were categorized into four groups: 18-24 (16.9%, n=65), 25-34 (72.7%, n=280), 35-44 (10.4%, n=40). The mean age group suggests that the majority of respondents fall into the 25-34 age range, with a standard deviation reflecting the spread across all age groups. Employees in the 25-34 age group showed a positive perception towards financial technology and cybersecurity, indicating that younger professionals are more inclined to adopt and support these innovations.

Educational qualifications ranged from high school to doctorate or professional degrees. The majority hold a master's degree (50.1%, n=193), followed by bachelor's degree holders (40.3%, n=155), high school graduates (8.6%, n=33), and doctorate or professional degree holders (1.0%, n=4). The mean educational qualification is aligned with a high level of education, and the standard deviation indicates a significant skew towards higher education. This suggests that employees with higher educational qualifications have a positive perception of financial technology and cybersecurity, valuing its importance in their roles.

Job positions were categorized into entry-level/staff (23.6%, n=91), mid-level/manager (59.2%, n=228), and senior management (17.1%, n=66). The mean score for job position reflects a dominance of mid-level managers, with a standard deviation showing the distribution across various positions. Mid-level managers displayed a particularly positive perception towards financial technology and cybersecurity, likely due to their responsibility in implementing and overseeing these systems.

Years of experience were divided into four categories: 0-5 years (47.0%, n=181), 6-10 years (41.3%, n=159), 11-15 years (8.6%, n=33), and 16 and above (3.1%, n=12). The mean years of experience suggest that most respondents are relatively early in their careers, with the standard deviation indicating a wide range of experience levels. Employees with 6-10 years of experience showed the most positive perception towards financial technology and cybersecurity, highlighting their growing familiarity and comfort with these technologies as they advance in their careers.

Respondents were from various departments: operations (61.0%, n=235), IT/technology (21.0%, n=81), risk management (13.5%, n=52), and compliance (4.4%, n=17). The mean departmental distribution is heavily skewed towards operations, with a standard deviation showing lesser representation in other departments. IT/technology department employees exhibited the most positive perception towards financial technology and cybersecurity, as these areas are integral to their daily responsibilities and expertise.

The types of banks represented included private banks (28.6%, n=110), government banks (28.6%, n=110), and joint venture banks (42.9%, n=165). The mean type of bank indicates a higher proportion of joint venture banks, with a standard deviation that demonstrates varied representation.

4.1.2 Status of Cybersecurity in Nepal

In this section, the perceptions of bank employees regarding the status of cybersecurity in Nepal are analyzed.

Table 4

Status of Cybersecurity in Nepal

Status		Frequency	Percent
Have you received any specific training on cybersecurity?	Yes	279	72.50
	No	106	27.50
On a scale of 1 to 5, how would you rate your level of familiarity with financial technology (FinTech)?	Very Low	2	0.50
	Low	25	6.50
	Neutral	113	29.40
	High	219	56.90
	Very High	26	6.80
How would you rate the overall preparedness of your bank against cybersecurity threats specific to the banking sector in Nepal?	Very prepared	58	15.10
	Prepared	219	56.90
	Neutral	86	22.30
	Unprepared	22	5.70
What is the frequency of cybersecurity training provided to employees in your bank?	Monthly	84	21.80
	Quarterly	181	47.00
	Bi-annually	100	26.00
	Annually	20	5.20
Has your bank implemented any of the following Nepal-specific cybersecurity guidelines or frameworks?	Guidelines issued by Nepal Rastra Bank (NRB)	139	36.10
	Local industry best practices	146	37.90
	International standards	74	19.20
	None of the above	26	6.80
What are the most common types of cybersecurity incidents your bank has faced in the last year?	Unauthorized access attempts	108	28.10
	Phishing attacks targeting Nepali customers	194	50.40
	Fraudulent transactions	42	10.90
	Data breaches involving customer information	41	10.60
How does your bank ensure compliance with cybersecurity regulations set forth by Nepal Rastra Bank (NRB)?	Regular audits and compliance checks	116	30.10
	Implementation of NRB-mandated security measures	199	51.70
	Staff training and awareness programs	29	7.50
	Third-party security assessments	41	10.60

Source: Field survey, 2024

Table 4 prescribes the status of financial technology and cybersecurity in Nepal. Out of the 385 respondents, 279 (72.50%) reported receiving specific training on cybersecurity, while 106 (27.50%) indicated otherwise. This high percentage suggests that banks prioritize educating their employees on cybersecurity protocols and practices to enhance their understanding and preparedness against cyber threats. The structured training programs likely cover various aspects of cybersecurity, including threat detection, incident response, and security best practices, thereby contributing to a more robust cybersecurity posture within the banking sector.

In case of how employee rate the level of familiarity with finance technology, following results has drawn. Very Low (2, 0.50%), Low (25, 6.50%), Neutral (113, 29.40%), High (219, 56.90%), and Very High (26, 6.80%). Notably, a significant proportion of respondents rated their familiarity with FinTech as High, indicating a substantial level of awareness and proficiency in FinTech concepts and technologies. This suggests that employees in Nepalese banks are well-equipped to engage with and leverage technological innovations in the financial sector to drive efficiency and innovation.

On the other hand employee perceived that whether bank are prepared for cybersecurity threats, following results has come. Very prepared (58, 15.10%), Prepared (219, 56.90%), Neutral (86, 22.30%), and Unprepared (22, 5.70%). This shows employees' perceptions of their banks' readiness to counter cybersecurity threats specific to the banking sector in Nepal, reflecting varying degrees of preparedness. . A substantial portion of respondents indicated that their banks were Prepared to counter cybersecurity threats, while only a small percentage (5.70%) felt that their banks were Unprepared. This suggests that banks in Nepal are actively implementing cybersecurity measures to mitigate risks and protect against potential cyber threats, contributing to the overall resilience of the banking sector.

Reported frequencies include Monthly (84, 21.80%), Quarterly (181, 47.00%), Bi-annually (100, 26.00%), and Annually (20, 5.20%). The majority of respondents indicated that cybersecurity training sessions are conducted Quarterly, highlighting a proactive approach to educating employees on cybersecurity best practices and protocols. This regular training regime ensures that employees stay updated on the latest cybersecurity threats and trends, thereby enhancing the overall security posture of banks in Nepal.

Respondents indicated adherence to various cybersecurity guidelines, Guidelines issued by Nepal Rastra Bank (NRB) (139, 36.10%), Local industry best practices (146, 37.90%), International standards (74, 19.20%), and None of the above (26, 6.80%). Respondents indicated adherence to various cybersecurity guidelines, including those issued by Nepal Rastra Bank (NRB), local industry best practices, and international standards. This demonstrates banks' commitment to aligning with regulatory mandates and industry standards to enhance cybersecurity governance and regulatory compliance. Overall, the variable reflects the comprehensive approach adopted by banks to strengthen cybersecurity measures and safeguard against cyber threats in Nepal's banking sector.

4.1.3 Descriptive Statistics of Financial Technology and Cyber Security

In this section, the descriptive statistics of various financial technology dimensions, such as self-efficacy, information security, technological culture, competence and skill, and cybersecurity, have been analyzed. This analysis provides a detailed overview of the respondents' perceptions and experiences related to these key areas, highlighting the current state and effectiveness of financial technology practices and security measures within the banking sector.

Table 5

Summary of Descriptive Statistics

Code	Variables	Mean	S.D.
SEF	Self-Efficacy	3.662	0.684
INS	Information Security	3.895	0.497
TEC	Technological Culture	3.893	0.413
CAS	Competence and Skill	3.724	0.561
CYS	Cyber security	3.983	0.381

Source: Field survey, 2024

Table 5 presents the descriptive study of employee perceptions towards financial technology and cybersecurity in commercial banks in Nepal. The table provides a summary of key variables, including self-efficacy (SEF), information security (INS), technological culture (TEC), competence and skill (CAS), and cybersecurity (CYS), along with their respective mean scores and standard deviations. This descriptive analysis aims to shed light on the prevailing perceptions and attitudes of bank employees towards various aspects of financial technology and cybersecurity within their organizations.

With a mean score of 3.983 (SD = 0.381), Cybersecurity stands out as the variable with the highest perception among respondents. This suggests that employees in commercial banks in Nepal perceive cybersecurity measures to be robust and effective in safeguarding against potential threats and vulnerabilities. The relatively low standard deviation indicates a high level of consensus among respondents regarding the importance and effectiveness of cybersecurity practices within their organizations.

Information Security has a mean score of 3.895 (SD = 0.497). This indicates that respondents perceive their organizations to have strong measures in place to ensure the confidentiality, integrity, and availability of information assets. While slightly lower than Cybersecurity, the high mean score suggests a significant level of confidence in the information security protocols implemented within commercial banks in Nepal.

The mean score for Technological Culture is 3.893 (SD = 0.413), reflecting a positive perception among respondents regarding the organizational culture surrounding technology adoption and innovation. This suggests that employees perceive their organizations to foster an environment that values and encourages the use of technology to enhance efficiency, productivity, and competitiveness in the banking sector.

Competence and Skill received a mean score of 3.724 (SD = 0.561), indicating a moderately high perception among respondents regarding their competency and skill levels in utilizing financial technology and cybersecurity tools and techniques. While the mean score is slightly lower compared to other variables, the standard deviation suggests some variability in respondents' perceptions, with potential areas for improvement in terms of skill development and training initiatives.

Self-Efficacy has the lowest mean score among the variables, with a mean of 3.662 (SD = 0.684). This suggests that respondents exhibit a slightly lower level of confidence in their self-efficacy related to financial technology and cybersecurity. The higher standard deviation indicates greater variability in respondents' perceptions, highlighting potential challenges in building confidence and empowering employees to effectively utilize technology in their roles.

The descriptive study reveals generally positive perceptions among respondents towards financial technology and cybersecurity in commercial banks in Nepal. While there are areas for improvement, such as enhancing self-efficacy and confidence levels, the findings indicate a strong foundation and readiness within the banking sector to embrace

and address the challenges and opportunities presented by advancements in technology and cybersecurity.

4.1.4 Correlation Analysis

In this section, the correlations between various financial technology dimensions, such as self-efficacy, information security, technological culture, competence and skill, and cybersecurity, have been analyzed. This analysis examines the relationships and interdependencies among these dimensions, providing insights into how they collectively influence the overall cybersecurity posture within the banking sector.

Table 6

Correlation Analysis

Variables		SEF	INS	TEC	CAS	CYS
SEF	Pearson Correlation	1				
	Sig. (2-tailed)					
INS	Pearson Correlation	.826**	1			
	Sig. (2-tailed)	0.000				
TEC	Pearson Correlation	.628**	.744**	1		
	Sig. (2-tailed)	0.000	0.000			
CAS	Pearson Correlation	.905**	.813**	.702**	1	
	Sig. (2-tailed)	0.000	0.000	0.000		
CYS	Pearson Correlation	.543**	.648**	.742**	.584**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	

Source: Appendix IV

Table 6 presents the correlation between the independent variables, namely self-efficacy (SEF), information security (INS), technological culture (TEC), competence and skill (CAS), and the dependent variable cybersecurity (CYS). The correlation analysis reveals a moderate positive correlation between self-efficacy and cybersecurity ($r = 0.543$, $p < 0.05$). This indicates that there is a statistically significant, moderate positive relationship between self-efficacy and cybersecurity 5 percent level of significance. Bank employees who perceive themselves as more capable and confident in their abilities tend to have more positive perceptions of cybersecurity readiness within their organizations.

A strong positive correlation is observed between information security and cybersecurity ($r = 0.648$, $p < 0.05$). This suggests that there is a statistically significant, strong positive relationship between perceived information security and cybersecurity 5 percent level of

significance. Bank employees who perceive higher levels of information security within their organizations also tend to have more positive perceptions of cybersecurity readiness.

The analysis indicates a strong positive correlation between technological culture and cybersecurity ($r = 0.742$, $p < 0.05$). This implies that there is a statistically significant, strong positive relationship between technological culture and cybersecurity at 5 percent level of significance. Bank organizations with a positive technological culture tend to have more positive perceptions of cybersecurity readiness among their employees.

There is a moderate positive correlation between competence and skill and cybersecurity ($r = 0.584$, $p < 0.05$). This suggests that there is a statistically significant, moderate positive relationship between perceived competence and skill and cybersecurity 5 percent level of significance.

4.1.5 Regression Analysis

In this section, a multivariate regression analysis has been conducted to examine the impact of various financial technology dimensions, such as self-efficacy, information security, technological culture, competence, and skill, on cybersecurity.

Table 7

Model Summary of Regression Model

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.756	0.571	0.567	0.25082

Source: Appendix V

Table 7 presents the model summary of the regression model. The model shows an overall significant relationship ($R = 0.756$, $p < 0.05$) between the predictors, including CAS (Competence and Skill), TEC (Technological Culture), INS (Information Security), SEF (Self-Efficacy), and the dependent variable CYS (Cybersecurity). The R-square value of 0.571 indicates that approximately 57.1% of the variance in cybersecurity can be explained by the predictors in the model. The adjusted R-square value (0.567) considers the number of predictors and provides a more accurate estimate of the variance explained.

Table 8

ANOVA Table of Regression Model

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.867	4	7.967	126.639	0.00
	Residual	23.905	380	0.063		
	Total	55.772	384			

Source: Appendix V

Table 8 provides the ANOVA table of the regression model. The significance value (Sig.) of the F-test is 0.00, indicating that the overall regression model is statistically significant at the 5% level of significance. This suggests that at least one of the predictors (CAS, TEC, INS, SEF) significantly contributes to the prediction of the dependent variable CYS (Cybersecurity). Therefore, the model is deemed fit for analysis as the significance value is less than 0.05.

Table 9

Beta Coefficient of Regression Model

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.248	0.126		9.904	0.000
	SEF	0.343	0.048	0.006	0.071	0.009
	INS	0.166	0.053	0.217	3.109	0.002
	TEC	0.536	0.049	0.581	10.947	0.000
	CAS	0.373	0.059	0.005	0.064	0.009

Source: Appendix V

Table 9 displays the unstandardized coefficients, standardized coefficients (Beta), and significance values (Sig.) of the independent variables on the dependent variable. For the variable SEF (Self-Efficacy), the unstandardized coefficient (B) is 0.343, and the standardized coefficient (Beta) is 0.006. The significance value is 0.009, which is significant at the 5% level, suggesting that for every one-unit increase in self-efficacy, there is a corresponding increase in cybersecurity.

Regarding INS (Information Security), the unstandardized coefficient is 0.166, and the standardized coefficient is 0.217. The significance value is 0.002, which is significant at

the 5% level. This implies that higher levels of information security are associated with higher cybersecurity.

For TEC (Technological Culture), the unstandardized coefficient is 0.536, and the standardized coefficient is 0.581. The significance value is 0, indicating high significance at the 5% level. This suggests that a positive technological culture is strongly associated with higher levels of cybersecurity.

Regarding CAS (Competence and Skill), the unstandardized coefficient is 0.373, and the standardized coefficient is 0.005. The significance value is 0.009, which is significant at the 5% level. This implies that greater competence and skill are associated with higher levels of cybersecurity.

These findings suggest that self-efficacy, information security, technological culture, and competence and skill all have significant positive impacts on cybersecurity. Organizations that focus on enhancing these factors are likely to experience improved cybersecurity outcomes, contributing to a safer and more secure environment for their operations.

4.1.5 Testing of Hypothesis

Table 10
Testing of Hypothesis

S.N.	Hypothesis	Tools Used for Hypothesis Testing	Correlation Coefficient	Sig.(P) Value	Accept
1	There is a significant positive relationship between self-efficacy and the effectiveness of cybersecurity measures within commercial banks.	Correlation Analysis	0.543	0.000	Accept
2	There is a significant positive relationship between information security culture and the effectiveness of cybersecurity measures within commercial banks.	Correlation Analysis	0.648	0.000	Accept
3	There is a significant positive relationship between technological competence and the effectiveness of cybersecurity measures within commercial banks.	Correlation Analysis	0.742	0.000	Accept

4	There is a significant positive relationship between skill and the effectiveness of cybersecurity measures within commercial banks.	Correlation Analysis	0.585	0.000	Accept

Hypothesis I

There is a significant positive relationship between self-efficacy and the effectiveness of cybersecurity measures within commercial banks.

Table 10 presents the results of the correlation analysis, showing a correlation coefficient of 0.543 and a p-value of 0.000. The p-value is less than the predetermined significance level of 0.05, indicating strong statistical significance. Therefore, Hypothesis I is accepted, suggesting that there is indeed a significant positive relationship between self-efficacy and the effectiveness of cybersecurity measures within commercial banks.

Hypothesis II

There is a significant positive relationship between information security culture and the effectiveness of cybersecurity measures within commercial banks.

As depicted in Table 10, the correlation analysis yielded a correlation coefficient of 0.648 with a p-value of 0.000. Since the p-value is lower than the predetermined significance level of 0.05, Hypothesis II is accepted. This implies that there exists a significant positive relationship between information security culture and the effectiveness of cybersecurity measures within commercial banks.

Hypothesis III

There is a significant positive relationship between technological competence and the effectiveness of cybersecurity measures within commercial banks.

Table 10 displays the results of the correlation analysis, showing a correlation coefficient of 0.742 and a p-value of 0.000. With the p-value below the predetermined significance level of 0.05, Hypothesis III is accepted. This indicates a significant positive relationship between technological competence and the effectiveness of cybersecurity measures within commercial banks.

Hypothesis IV

There is a significant positive relationship between skill and the effectiveness of cybersecurity measures within commercial banks.

As indicated in Table 10, the correlation analysis revealed a correlation coefficient of 0.585 and a p-value of 0.000. Since the p-value is less than the predetermined significance level of 0.05, Hypothesis IV is accepted. This suggests that there is a significant positive relationship between skill and the effectiveness of cybersecurity measures within commercial banks.

4.1.6 Major Findings

- 53.8% of the respondents are male (n=207), while 46.2% are female (n=178).
- The majority of respondents fall into the 25-34 age group (72.7%, n=280), followed by 18-24 (16.9%, n=65) and 35-44 (10.4%, n=40).
- Regarding educational qualifications, 50.1% hold a master's degree (n=193), 40.3% are bachelor's degree holders (n=155), 8.6% are high school graduates (n=33), and only 1.0% have doctorate or professional degrees (n=4).
- Job positions are primarily held by mid-level managers (59.2%, n=228), followed by entry-level/staff (23.6%, n=91), and senior management (17.1%, n=66).
- In terms of experience, most respondents have 0-5 years of experience (47.0%, n=181), followed by 6-10 years (41.3%, n=159), 11-15 years (8.6%, n=33), and 16 years and above (3.1%, n=12).
- The distribution across departments shows a dominance of operations (61.0%, n=235), followed by IT/technology (21.0%, n=81), risk management (13.5%, n=52), and compliance (4.4%, n=17).
- Among the types of banks represented, joint venture banks have the highest representation (42.9%, n=165), followed by private banks (28.6%, n=110), and government banks (28.6%, n=110).
- Significant proportion of respondents (72.50%) reported receiving specific training on cybersecurity, highlighting a strong emphasis on employee education and preparedness within Nepalese banks.
- The majority of respondents (56.90%) rated their familiarity with financial technology (FinTech) as High, indicating a substantial level of awareness and proficiency in FinTech concepts and technologies among bank employees.

- The perception of banks' preparedness against cybersecurity threats was largely positive, with 56.90% of respondents indicating that their banks were Prepared. This suggests active implementation of cybersecurity measures within the banking sector in Nepal.
- Quarterly cybersecurity training sessions were the most common, with 47.00% of respondents indicating this frequency, demonstrating a proactive approach to keeping employees informed about cybersecurity best practices.
- Adherence to cybersecurity guidelines was evident, with respondents indicating compliance with guidelines issued by Nepal Rastra Bank (NRB), local industry best practices, and international standards. This reflects a comprehensive approach to cybersecurity governance and regulatory compliance within Nepalese banks.
- Overall, the findings suggest that Nepalese banks prioritize cybersecurity education and preparedness, demonstrate a strong familiarity with FinTech concepts, and actively implement cybersecurity measures aligned with regulatory standards and industry best practices.
- Cybersecurity is perceived most positively among respondents, with a mean score of 3.983 and a low standard deviation, indicating robust measures against threats.
- Information Security also receives high perception scores (mean = 3.895), suggesting strong confidence in safeguarding information assets.
- Technological Culture is positively perceived (mean = 3.893), indicating an organizational environment that values technology adoption and innovation.
- Competence and Skill are moderately perceived (mean = 3.724), with some variability suggesting room for improvement in skill development.
- Self-Efficacy has the lowest mean score (3.662), indicating lower confidence levels among respondents, highlighting a potential area for empowerment and training.
- Overall, the study reflects generally positive perceptions towards financial technology and cybersecurity, indicating a readiness within the banking sector to address technological advancements and security challenges.

- A moderate positive correlation (r = 0.543) exists between self-efficacy and cybersecurity, indicating that employees who feel more capable tend to perceive higher levels of cybersecurity readiness within their organizations.
- A strong positive correlation (r = 0.648) is observed between information security and cybersecurity, implying that employees who perceive higher information security levels also tend to have more positive perceptions of cybersecurity readiness.
- There is a strong positive correlation (r = 0.742) between technological culture and cybersecurity, suggesting that organizations fostering a positive technological culture tend to have more positive perceptions of cybersecurity readiness among their employees.
- A moderate positive correlation (r = 0.584) is found between competence and skill and cybersecurity, indicating that employees who perceive themselves as more competent and skilled in technology-related tasks tend to have more positive perceptions of cybersecurity readiness.
- The regression model shows an overall significant relationship (R = 0.756, $p < 0.05$) between the predictors (CAS, TEC, INS, SEF) and the dependent variable (CYS), indicating that the predictors collectively contribute to predicting cybersecurity readiness.
- The R-square value of 0.571 suggests that approximately 57.1% of the variance in cybersecurity can be explained by the predictors in the model, indicating a moderately strong predictive power of the model.
- The adjusted R-square value (0.567) provides a more accurate estimate of the variance explained, considering the number of predictors in the model.
- For the variable SEF (Self-Efficacy), the unstandardized coefficient (B) is 0.343, with a standardized coefficient (Beta) of 0.006. The significance value is 0.009, indicating significance at the 5% level, implying that higher self-efficacy is associated with increased cybersecurity readiness.
- INS (Information Security) shows an unstandardized coefficient of 0.166 and a standardized coefficient of 0.217. The significance value is 0.002, significant at

the 5% level. This implies that higher levels of information security correlate with improved cybersecurity.

- TEC (Technological Culture) exhibits an unstandardized coefficient of 0.536 and a standardized coefficient of 0.581, with a significance value of 0, highly significant at the 5% level, indicating that a positive technological culture is strongly associated with higher cybersecurity levels.
- CAS (Competence and Skill) displays an unstandardized coefficient of 0.373 and a standardized coefficient of 0.005, with a significance value of 0.009, significant at the 5% level. This implies that greater competence and skill relate to improved cybersecurity.
- Overall, these findings indicate that self-efficacy, information security, technological culture, and competence and skill significantly impact cybersecurity positively. Organizations focusing on enhancing these factors are likely to achieve better cybersecurity outcomes, fostering a safer operational environment.

4.2 Discussion

The study examining the current status of cybersecurity in commercial banks in Nepal reveals a commendable commitment to cybersecurity education and preparedness, emphasizing employee training and active implementation of cybersecurity measures aligned with regulatory standards. This aligns with Samoei and Gatobu (2024) findings in Kenyan commercial banks, emphasizing the significance of application security and IT governance in internet banking services. Similarly, Umoga et al. (2024) underscore the importance of proactive cybersecurity strategies and human factors awareness in financial technologies, echoing the emphasis on employee education and preparedness. However, Alsakini et al. (2024) focus on the impact of cybersecurity breaches on financial accounting statements, diverging from the emphasis on employee training and organizational preparedness. Farayola (2024) proposes innovative solutions integrating AI, Blockchain, and BI for banking security, aligning with the need for robust cybersecurity measures highlighted in the study. Choithani et al, (2024) delve into AI's role in cryptocurrency analysis, complementing the study's focus on technological advancements and cybersecurity in banking. Overall, the current study underscores the importance of employee education and proactive cybersecurity measures, aligning with

previous research emphasizing the critical role of technology and human factors in banking cybersecurity.

The study also aimed to examine the correlation between financial technology and cybersecurity in Nepalese commercial banks. Through correlation analysis, significant positive relationships were found between various factors like self-efficacy, information security, technological culture, competence, and skill with cybersecurity. These results suggest that employees' perceptions of their capabilities, the level of information security, organizational technological culture, and their competence and skill levels influence cybersecurity readiness. Hence, it's concluded that there exists a meaningful and positive relationship between financial technology and cybersecurity in Nepalese banks, emphasizing the need for supportive organizational environments and empowering employees to bolster cybersecurity measures. This aligns with findings from previous research, such as Umoga et al. (2024), which also emphasizes the importance of understanding cybersecurity challenges amidst the rapid evolution of financial technologies. Similarly, Farayola (2024) proposes integrating AI, Blockchain, and Business Intelligence (BI) to enhance banking security, echoing the importance of technological innovation highlighted in the Nepalese study. Additionally, Choithani et al. (2024) emphasize AI's role in addressing various aspects related to cryptocurrencies, supporting the notion of leveraging technology to enhance cybersecurity. However, while the Nepalese study focuses on the organizational environment and employee empowerment, other studies, such as Alsakini et al. (2024), delve into the impact of cybersecurity breaches on financial statements, offering insights into the direct consequences of cyber incidents. Overall, while there is alignment in recognizing the significance of technology and cybersecurity, each study offers unique insights into specific aspects of the complex relationship between financial technology and cybersecurity in the banking sector.

Additionally, this study investigated the impact of financial technology and cybersecurity in Nepalese commercial banks using regression analysis. It reveals that each independent variable - self-efficacy, information security, technological culture, and competence and skill - positively influences cybersecurity. Higher levels of these variables correlate with increased cybersecurity readiness, with technological culture having the strongest impact. The statistical significance at the 5% level underscores the importance of fostering a supportive organizational culture, improving information security measures, and

empowering employees to tackle cybersecurity challenges effectively within Nepal's banking sector. The findings of the study on the impact of financial technology and cybersecurity in Nepalese commercial banks align with several previous research works. Studies by Umoga et al. (2024) and Farayola (2024) underscore the importance of technological innovations, such as AI and Blockchain, in addressing cybersecurity challenges, resonating with the emphasis on fostering a supportive organizational culture and enhancing information security measures in the Nepalese context. Similarly, Alsakini et al. (2024) and Choithani et al. (2024) delve into the consequences of cybersecurity breaches and advocate for technological solutions, aligning with the Nepalese study's focus on the positive impact of self-efficacy, information security, and technological culture on cybersecurity readiness. Moreover, Despotovic et al. (2023) highlight the significance of user awareness and employee training in mitigating cyber threats, which complements the emphasis on empowering employees with necessary skills in the Nepalese study.

CHAPTER V
SUMMARY AND CONCLUSION

This chapter encapsulates the culmination of the study's efforts by offering a comprehensive overview of the findings, conclusions, and implications. In the summary section, the key discoveries and contributions of the research are synthesized, emphasizing the significant relationships identified among various variables pertaining to financial technology and cybersecurity within Nepalese commercial banks. The conclusion segment underscores the broader implications of the study's outcomes, highlighting their relevance in enhancing the understanding of factors influencing cybersecurity readiness in banking institutions. Moreover, the chapter delves into theoretical and practical implications, elucidating how the research advances existing literature and provides actionable insights for policymakers, banking professionals, and cybersecurity practitioners. Through its cohesive narrative, this chapter serves as a pivotal point of reflection, consolidating the study's findings and paving the way for future research endeavors in the realm of financial technology and cybersecurity in Nepal's banking sector.

5.1 Summary

This study evaluates the transformative impact of financial technology (Fintech) on the financial services industry, ushering in a new era of convenience and accessibility through technological innovation. However, this advancement brings forth challenges, particularly in cybersecurity, as the digitization of financial services amplifies the risk of cyber threats. The intersection of Fintech and cybersecurity necessitates a delicate balance between innovation and security, requiring collaborative efforts from stakeholders to develop robust regulatory frameworks and enhance cybersecurity measures. Against this backdrop, the study focuses on the impact of Fintech adoption on the cybersecurity landscape of commercial banks in Nepal. The objectives include examining the current status of cybersecurity, analyzing the relationship between Fintech and cybersecurity, and assessing the overall impact of financial technology on commercial banks in Nepal. Through these objectives, the study aims to identify potential risks, vulnerabilities, and strategies to mitigate cyber threats, ultimately safeguarding financial institutions and their customers in Nepal's evolving digital landscape.

The literature review of this study encompasses a comprehensive analysis across three main categories: conceptual review, theoretical review, empirical review, and a discussion on research gaps. In the conceptual review, the study explores the transformative dynamics and challenges within the Fintech ecosystem, emphasizing the significant impact of Fintech innovations on the financial services industry and the concurrent implications for information security and cybersecurity. This section examines the intricate interplay between Fintech and information security, highlighting the imperative of safeguarding financial data and systems in the digital era, while also addressing emerging threats and vulnerabilities within the cybersecurity domain. Transitioning to the theoretical review, the study draws upon various theoretical frameworks, including systems theory, personality theory, risk expectations theory, and institutional theory, to provide insights into the complex dynamics of Fintech adoption and its ramifications on cybersecurity. By leveraging these theoretical lenses, the study elucidates individual and organizational behaviors, regulatory influences, and environmental factors shaping cybersecurity practices within Fintech firms and financial institutions. Subsequently, in the empirical review section, the study synthesizes existing empirical research on Fintech and cybersecurity, aiming to discern patterns, trends, and areas for further investigation. Finally, the research gap analysis critically evaluates the extant literature, identifying gaps, inconsistencies, and unexplored areas that necessitate further exploration to advance knowledge and inform policy initiatives in the evolving landscape of Fintech and cybersecurity.

This study employed both a descriptive research design and a causal-comparative research design to investigate financial technology's impact on cybersecurity in commercial banks within the Kathmandu Valley, Nepal. The population of interest comprises all employees in commercial banks in the Kathmandu Valley, and a sample size of 385 employees is selected using convenience sampling. Cochran's formula is applied to determine the sample size, resulting in 385 participants. The sample includes employees from various types of banks, including government banks, joint venture banks, and private banks, ensuring representation across different sectors. Data collection is conducted through structured questionnaire surveys, drawing on insights from previous literature and consultations with experts. The questionnaire is designed to capture relevant variables and factors identified in the literature, employing a five-point Likert scale to measure respondents' opinions and perceptions. This quantitative approach enables

rigorous analysis and interpretation of the data to address the research objectives and contribute to advancing knowledge in the field of financial technology and cybersecurity.

In this study, data collected from commercial banks in the Kathmandu Valley, Nepal, is analyzed using statistical software such as Microsoft Excel and SPSS. Descriptive statistics, correlation analysis, and multivariate regression models are employed as analytical tools to explore the relationship between financial technology (Fintech) adoption and cybersecurity measures. Descriptive statistics allow for the examination of central tendency and dispersion of data, providing insights into the current status of Fintech and cybersecurity in commercial banks. Correlation analysis is utilized to identify potential associations between Fintech adoption and cybersecurity measures, while multivariate regression models investigate the impact of Fintech on cybersecurity, controlling for other relevant factors. The research framework comprises independent variables including self-efficacy, information security, technological culture, competence, and skill, which represent individual and organizational attributes related to cybersecurity readiness. The dependent variable, cybersecurity, reflects the overall security posture of commercial banks and is influenced by the identified independent variables. Through this analysis, the study aims to provide comprehensive insights into the factors shaping cybersecurity practices and resilience in the Nepalese banking sector.

Based on the findings of this study, it can be concluded that the independent variables examined, including self-efficacy, information security, technological culture, and competence and skill, collectively serve as significant determinants of cybersecurity readiness in commercial banks in Nepal. The examination of the current status of cybersecurity revealed commendable efforts by Nepalese banks in prioritizing cybersecurity education and preparedness, indicating a strong commitment to addressing evolving threats. Additionally, the analysis of the relationship between financial technology and cybersecurity highlighted meaningful and positive correlations between various independent variables and cybersecurity, emphasizing the importance of fostering a supportive organizational environment and empowering employees to enhance cybersecurity measures. Furthermore, the regression analysis demonstrated that each independent variable had a significant and positive impact on cybersecurity, further substantiating their role as key determinants of cybersecurity readiness. Therefore, it can be concluded that the independent variables examined in this study collectively contribute to the overall cybersecurity posture of commercial banks in Nepal, underscoring the

importance of organizational culture, information security measures, and employee empowerment in effectively addressing cybersecurity challenges.

The findings of this study carry both practical and theoretical implications. Practically, it underscores the importance of enhancing cybersecurity measures in commercial banks, especially in the context of increasing adoption of financial technology. Theoretical implications include contributing to the understanding of the relationship between Fintech adoption and cybersecurity readiness. Recommendations include implementing robust cybersecurity protocols, fostering a culture of cybersecurity awareness, and investing in continuous training and education for employees to mitigate cyber threats effectively.

5.2 Conclusion

The first objective of this study is to examine the current status of cybersecurity in commercial banks in Nepal. Based on the findings, it can be concluded that Nepalese banks have demonstrated a commendable commitment to cybersecurity education and preparedness. A significant proportion of respondents reported receiving specific training on cybersecurity, indicating a strong emphasis on employee education and readiness within the banking sector. Additionally, the perception of banks' preparedness against cybersecurity threats reflects active implementation of cybersecurity measures aligned with regulatory standards. While there are positive perceptions regarding cybersecurity and information security, areas for improvement include enhancing self-efficacy levels among employees. Overall, the study suggests that Nepalese banks prioritize cybersecurity education and preparedness, but efforts should continue to empower employees and strengthen cybersecurity measures to effectively address evolving threats.

The second objective of this study is to analyze the relationship between financial technology and cybersecurity in commercial banks in Nepal. Based on the correlation analysis, it is evident that there are significant and positive relationships between various independent variables (self-efficacy, information security, technological culture, competence, and skill) and the dependent variable, cybersecurity. Specifically, self-efficacy, information security, technological culture, and competence and skill all demonstrate moderate to strong positive correlations with cybersecurity. These findings suggest that employees' perceptions of their own capabilities, the level of information security within their organizations, the technological culture fostered by their employers, and their competence and skill levels in handling technology-related tasks are all

important factors influencing cybersecurity readiness in Nepalese banks. Therefore, it can be concluded that there is a meaningful and positive relationship between financial technology and cybersecurity in commercial banks in Nepal, highlighting the importance of fostering a supportive organizational environment and empowering employees to enhance cybersecurity measures.

The third objective of this study is to analyze the impact of financial technology and cybersecurity in commercial banks in Nepal. Based on the regression analysis, it is evident that each independent variable (self-efficacy, information security, technological culture, and competence and skill) has a significant and positive impact on the dependent variable, cybersecurity. Specifically, higher levels of self-efficacy, information security, technological culture, and competence and skill are associated with increased cybersecurity readiness within commercial banks. The standardized coefficients indicate the strength of these relationships, with technological culture exhibiting the strongest impact followed by information security, self-efficacy, and competence and skill. Furthermore, the significance values at the 5% level indicate the statistical significance of these relationships. Overall, these findings underscore the importance of fostering a supportive organizational culture, enhancing information security measures, and empowering employees with the necessary skills and confidence to effectively address cybersecurity challenges within the banking sector in Nepal.

5.3 Implications

This study has both theoretical as well as practical implications.

5.3.1 Theoretical Implications

The findings of this study contribute significantly to the theoretical understanding of the relationship between financial technology (Fintech) and cybersecurity within the context of commercial banks in Nepal. By demonstrating the positive impact of variables such as self-efficacy, information security, technological culture, and competence and skill on cybersecurity readiness, the study enriches existing literature on Fintech and cybersecurity. It provides empirical evidence supporting the importance of organizational factors and employee capabilities in enhancing cybersecurity measures, thereby advancing theoretical frameworks in this domain. Moreover, the study highlights the need for further research to explore the nuanced dynamics and mechanisms underlying the

relationship between Fintech and cybersecurity, offering avenues for future theoretical development in the field.

5.3.2 Practical Implications

The practical implications of this study are profound for commercial banks in Nepal and beyond. By identifying key factors influencing cybersecurity readiness, such as organizational culture and employee competencies, the findings offer actionable insights for bank managers and policymakers to strengthen cybersecurity measures effectively. Practically, banks can prioritize investments in employee training programs to enhance technological skills and promote a culture of cybersecurity awareness. Additionally, organizational policies and practices should be aligned to foster a supportive environment that encourages proactive cybersecurity behaviors. By implementing these recommendations, banks can mitigate cyber risks more effectively, safeguard customer data, and maintain trust and confidence in the financial system, ultimately contributing to the resilience and sustainability of the banking sector.

REFERENCES

Adeyoju, F. I. P. (2019). Cybercrime and cybersecurity: Fintech's greatest challenges. *SSRN Journal*, *3*(4), 86-127.

Akintoye, R., Ogunode, O., Ajayi, M., & Ambibola, A. J. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance*, *10*(3), 643-652.

Al Duhaidahawi, H. M. K., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. (2020). The financial technology (Fintech) and cybersecurity: Evidence from Iraqi banks. *International Journal of Research in Business and Social Science (2147-4478)*, *9*(6), 123-133.

Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536.

Al-Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Harjan, S. A., & Shah, S. S. H. (2019). The Role of Financial Inclusion and Competitive Advantage: Evidence From Iraqi Islamic Banks. *International Journal of Economics and Financial Issues*, *9*(3), 193-199.

Al-Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science*, *5*(6), 123-133.

Alodhiani, A. A. B. (2023). Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review. *Arab Journal of Humanities and Social Sciences*, *12*(1), 1-29.

Alsakini, S. A. K., Alawawdeh, H. A., & Alsayyed, S. (2024). The Impact of Cybersecurity on the Quality of Financial Statements. *Applied. Mathematics*, *18*(1), 169-181.

Alshehadeh, A. R., & Al-Khawaja, H. A. (2022). Financial Technology as a Basis for Financial Inclusion and its Impact on Profitability: Evidence from Commercial Banks. *International Journal of Advances in Soft Computing & Its Applications*, *14*(2), 13-28.

Alt, R., Fridgen, G., & Chang, Y. (2024). The future of Fintech-Towards ubiquitous financial services. *Electronic Markets*, *34*(1), 3-18.

Amenta, E., & Ramsey, K. M. (2010). Institutional theory. *Handbook of Politics: State and Society in Global Perspective*, *12*(3), 15-39.

Amissah, M., Gannon, T., & Monat, J. (2020). What is systems thinking? Expert perspectives from the WPI systems thinking colloquium. *Journal of Business*, *3*(4), 1-19.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in human behavior*, *26*(5), 857-869.

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The dark side of digital financial transformation: The new risks of fintech and the rise of techrisk. *UNSW Law Research Paper*, *13(*3), 19-89.

Callen-Naviglia, J., & James, J. (2018). Finttech Regteech and the Importance of Cybersecurity.. *Issues in Information Systems*, *19*(3), 1-14.

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on Bitcoin, crypto currency and banking system. *Annals of Data Science*, *11*(1), 103-135.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208.

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cyber security in Fintech. In Digital transformation of the financial industry: approaches and applications. *Springer International Journal, 1*(4), 255-272.

Didenko, A. N. (2020). Cybersecurity regulation in singapore's financial sector: protecting Fintech 'Ants' in a jungle full of 'Elephants'. *UNSW Law Research Paper*, 4(3), 20-45.

Diemers, D., Lamaa, A., Salamat, J., & Steffens, T. (2015). Developing a FinTech ecosystem in the GCC. *Dubai: Strategy*, *3*(3), 1-16.

Dung, M. T., & Do Khanh Van, N. G. B. Financial Technology in Commercial Banks: Situation and Solutions. *International Research Journal of Economics and Management Studies IRJEMS*, *2*(3), 23-34.

Ebrahim, R., Kumaraswamy, S., & Abdulla, Y. (2021). Fintech in banks: opportunities and challenges. *Innovative Strategies for Implementing Fintech in Banking*, *3*(2), 100-109.

Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, *6*(4), 501-514.

Firmansyah, E. A., & Anwar, M. (2019, January). Islamic financial technology (FINTECH): its challenges and prospect. In *Achieving and Sustaining SDGs 2018 Conference: Harnessing the Power of Frontier Technology to Achieve the Sustainable Development Goals (ASSDG 2018)* (pp. 52-58). Atlantis Press.

Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications*, *103*(4), 262-273.

Gaur, L., Afaq, A., Arora, G. K., & Khan, N. (2023). Artificial intelligence for carbon emissions using system of systems theory. *Ecological Informatics*, *7*(3), 102-165.

Gholami, M., Ghafari Ashtiani, P., Zanjirdar, M., & Haji, G. (2023). Investigating the effect of fintech implementation components in the banking industry of Iran. *Advances in Mathematical Finance and Applications*, *8*(2), 625-643.

Giri, S., & Shakya, S. (2020). High risk of cybercrime, threat, attack and future challenges in Nepal. *International Journal of Computer Sciences and Engineering*, *8*(2), 46-51.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.

Jasur, A. (2023). Cybersecurity and risk management in the financial sector. *International Bulletin of Young Scientist*, *1*(1), 1-19.

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *2*(3), 122-137.

Jayalath, J. A. R. C., & Premaratne, S. C. (2021). Analysis of key digital technology infrastructure and cyber security consideration factors for Fintech companies. *International Journal of Research Publications*, *84*(1), 128-135.

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). *Understanding Cybersecurity Management in Fintech*. Springer International Publishing.

Kondratyeva, M. N., Svirina, D. D., & Tsvetkov, A. I. (2021, February). The role of information technologies in ensuring banking security. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1047, No. 1, p. 012069). IOP Publishing.

Kryparos, G. (2018). Information security in the realm of FinTech. In *The Rise and Development of FinTech* (pp. 43-65). Routledge.

Kuzmina-Merlino, I., & Saksonova, S. (2018). The knowledge and competencies required for the fintech sector. *New Challenges of Economic and Business Development–2018: Productivity and Economic Growth*, *11*(3), 387-398.

Lala, G. (2014). The emergence and development of the technology acceptance model (TAM). *Marketing from Information to Decision*, *8*(7), 149-160.

Laurent, D., & Sinz, R. (2019). FinTech: The role of Perceived cybersecurity and Organizational trust. *Umeå School of Business, Economics and Statistics*, *1*(1), 1-110

Lee, M. K., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of electronic commerce*, *6*(1), 75-91.

Lee, Y. K. (2021). Impacts of digital technostress and digital technology self-efficacy on Fintech usage intention of Chinese Gen Z consumers. *Sustainability*, *13*(9), 50-77.

Maharjan, R., & Chatterjee, J. M. (2019). Framework for minimizing cyber security issues in banking sector of Nepal. *LBEF Research Journal of Science, Technology and Management*, *1*(1), 82-98.

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters?. *International Journal of Financial Engineering*, *8*(02), 215-229.

Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R. (2020). Conceptualising cybersecurity risk of fintech firms and banks sustainability. *Journal of Business, 3*(4), 15-45.

Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25*(4), 422-434.

Nuyens, H. (2019). How disruptive are Fintech and digital for banks and regulators?. *Journal of risk management in financial institutions*, *12*(3), 217-222.

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *Journal of Business, 3*(3), 12-23.

Philippon, T. (2016). The Fintech Opportunity. National Bureu of Economic research, 8(3), 6-10.

Roush, J. E. (2007). The expectations theory works for monetary policy shocks. *Journal of monetary Economics*, *54*(6), 1631-1643.

Salim, H. M. (2014). *Cyber safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks.* An Unpublished Master's Degree Dissertation, Submited of Office of Dean, Faculty of Information Technology, Massachusetts Institute of Technology.

Samoei, P. C., & Gatobu, P. (2024). Cybersecurity and Performance of Internet Banking Services in Commercial Bank in Nairobi City Country, Kenya. *International Journal of Social Sciences Management and Entrepreneurship (IJSSME)*, *8*(1), 23-45.

Savage, S., & Schneider, F. B. (2009). Security is not a commodity: The road forward for cybersecurity research. *May Journal*, *31(3)*, 120-141.

Șcheau, M. C., Rangu, C. M., Popescu, F. V., & Leu, D. M. (2022). Key pillars for Fintech and cybersecurity. *Acta Universitatis Danubius. Œconomica*, *18*(1), 1-19.

Shah, S. S. H., Xinping, X., Khan, M. A., & Harjan, S. A. (2018). Investor and manager overconfidence bias and firm value: Micro-level evidence from the Pakistan equity market. *International Journal of Economics and Financial Issues*, *8*(5), 190-223.

Shrestha, S. (2020). Lessons Nepal can learn from the UK in Data and Cyber Security. *Promoting cultural change in engineering practices for the Development of Nepal: Learning from the UK*, *3*(2), 4-13.

Singh, S., Sahni, M. M., & Kovid, R. K. (2020). What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model. *Management Decision*, *58*(8), 1675-1697.

Smith, K. J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, *46*(6), 833-848.

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime–realities and challenges. *Accounting and Management Information Systems*, *16*(4), 610-632.

Stanikzai, A. Q., & Shah, M. A. (2021, December). Evaluation of cyber security threats in banking systems. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI), 2(1),* 1-4.

Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845-851.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309.

Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, *11*(1), 1810-1817.

Vasiljeva, T., & Lukanova, K. (2016). Commercial banks and FINTECH companies in the digital transformation: Challenges for the future. *Journal of Business Management*, *11*(3), 24-38.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security*, *26*(1), 2-9.

Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice*, *11*(2), 27-53.

Williams, E. E., & Findlay III, M. C. (1986). Risk and the role of failed expectations in an uncertain world. *Journal of Post Keynesian Economics*, *9*(1), 32-47.

Wu, Z., & Liu, C. J. (2022). Study on decision optimization of emergency investment plan based on expectation theory. *Computational Social Science*, *3(*4), 230-236.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly*, 229-239.

APPENDICES

Appendix I: Questionnaire

Dear Sir/Mam,

I kindly request your participation in my Master's Degree Dissertation focusing on the relationship between financial technology (FinTech) and cybersecurity in commercial banks in Nepal. Your valuable insights will contribute to enhancing our understanding of this critical area and aid in the development of effective cybersecurity strategies within the banking sector.

Your responses will remain confidential and will be used solely for research purposes. Your participation is voluntary, and you may withdraw from the survey at any time.

Thank you for your time and cooperation.

Sincerely,

Susma Khatiwada

Part I Demographic Profile

Please put a tick mark (✓) in the box in an appropriate option for each of the following.

1. Name (Optional):
2. Gender:
   - Male
   - Female
3. Age:
   - 18-24
   - 25-34
   - 35-44
   - 45-54
   - 55 or above
4. Educational Qualification:
   - High School
   - Bachelor's Degree
   - Master's Degree

- Doctorate or Professional Degree

5. Job Position:
   - Entry-level/Staff
   - Mid-level/Manager
   - Senior Management
6. Years of Experience in Banking Industry:
   - 0-5
   - 6-10
   - 11-15
   - 16 or above
7. Department/Division:
   - Operations
   - IT/Technology
   - Risk Management
   - Compliance
8. Type of Bank:
   - Private Bank
   - Government Bank
   - Joint Venture Bank
9. Have you received any specific training on cybersecurity?
   - Yes
   - No
10. On a scale of 1 to 5, how would you rate your level of familiarity with financial technology (FinTech)? (1 - Very Low, 5 - Very High)

-1

-2

-3

-4

-5

11. How would you rate the overall preparedness of your bank against cybersecurity threats specific to the banking sector in Nepal?
    Very prepared
    Prepared
    Neutral
    Unprepared
    Very unprepared
12. What is the frequency of cybersecurity training provided to employees in your bank?

Monthly
Quarterly
Bi-annually
Annually

13. Has your bank implemented any of the following Nepal-specific cybersecurity guidelines or frameworks?
Guidelines issued by Nepal Rastra Bank (NRB)
Local industry best practices
International standards
None of the above

14 What are the most common types of cybersecurity incidents your bank has faced in the last year?
Unauthorized access attempts
Phishing attacks targeting Nepali customers
Fraudulent transactions
Data breaches involving customer information

15. How does your bank ensure compliance with cybersecurity regulations set forth by Nepal Rastra Bank (NRB)?
Regular audits and compliance checks
Implementation of NRB-mandated security measures
Staff training and awareness programs
Third-party security assessments

Part II Core Questions about financial technology (FinTech) and cybersecurity

Source: Laurent and Sinz (2019) Al-Duhaidahawi et al. (2020) and Javaheri et al. (2023)

Please put a tick mark (✓) in the box in an appropriate option for each of the following.

Self-Efficacy	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1. I feel confident in my ability to identify cyber threats and vulnerabilities.					
2. I believe I have the necessary skills to respond effectively to cyber attacks.					
3. I am confident in my ability to implement cybersecurity measures effectively.					
4. I feel empowered to take proactive measures to enhance cybersecurity in my bank.					

5. I believe my actions contribute significantly to improving cybersecurity in my bank.					
6. I am confident in my ability to communicate cybersecurity risks effectively to colleagues and stakeholders.					
7. I believe that my proactive approach to cybersecurity contributes positively to the overall security posture of my bank.					
Information Security	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1. I am aware of the importance of protecting sensitive information in my bank.					
2. I adhere to security policies and procedures to safeguard confidential data.					
3. I regularly update my knowledge on information security best practices.					
4. I am vigilant about potential security threats and risks in my work environment.					
5. I take proactive measures to prevent data breaches and unauthorized access to information.					
6. I understand the potential consequences of data breaches and unauthorized access to sensitive information in my bank.					
7. I actively participate in information security training programs to enhance my knowledge and skills in safeguarding data.					
Technological Culture	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1. There is a culture of embracing technology advancements in my bank.					
2. Employees are encouraged to adopt and adapt to new technologies					

in their work.					
3. There are opportunities for continuous learning and training on technological tools and systems.					
4. Technology is viewed as a strategic asset that enhances bankal effectiveness.					
5. Innovation and creativity are valued and promoted within the technological landscape of the bank.					
6. Technology-driven innovation is encouraged and supported by leadership within my bank.					
7. There is a culture of collaboration and knowledge sharing regarding technological advancements and their implications for cybersecurity.					
Competence and Skill	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1. I possess the necessary technical skills to effectively manage cybersecurity systems.					
2. I receive adequate training and support to enhance my cybersecurity competencies.					
3. My bank invests in developing the skills of its employees in cybersecurity.					
4. I feel confident in my ability to troubleshoot and resolve cybersecurity issues.					
5. I continuously seek opportunities to improve my cybersecurity knowledge and skills.					
6. I am proficient in using cybersecurity tools and technologies to mitigate risks effectively.					
7. Continuous professional development opportunities are provided to enhance employees' cybersecurity competencies and skills.					

Cybersecurity	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1. My bank prioritizes cybersecurity as a fundamental aspect of its operations.					
2. There are robust cybersecurity measures in place to protect sensitive information.					
3. I feel confident in the cybersecurity measures implemented by my bank.					
4. Cybersecurity is integrated into the overall business strategy of my bank.					
5. My bank regularly evaluates and updates its cybersecurity protocols to address emerging threats.					
6. My bank has established clear policies and procedures for incident response and breach management.					
7. I feel assured that my bank prioritizes cybersecurity investments to stay ahead of evolving threats and vulnerabilities.					

Appendix II: Frequency Table

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	207	53.8	53.8	53.8
	Female	178	46.2	46.2	100.0
	Total	385	100.0	100.0	

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	65	16.9	16.9	16.9
	25-34	280	72.7	72.7	89.6
	35-44	40	10.4	10.4	100.0
	Total	385	100.0	100.0	

Educational Qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	33	8.6	8.6	8.6
	Bachelor's Degree	155	40.3	40.3	48.8
	Master's Degree	193	50.1	50.1	99.0
	Doctorate or Professional Degree	4	1.0	1.0	100.0
	Total	385	100.0	100.0	

Job Position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Entry-level/Staff	91	23.6	23.6	23.6
	Mid-level/Manager	228	59.2	59.2	82.9
	Senior Management	66	17.1	17.1	100.0
	Total	385	100.0	100.0	

Years of Experience in Banking Industry

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-5	181	47.0	47.0	47.0
	6-10	159	41.3	41.3	88.3
	11-15	33	8.6	8.6	96.9
	16 and above	12	3.1	3.1	100.0
	Total	385	100.0	100.0	

Department

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Operations	235	61.0	61.0	61.0
	IT/Technology	81	21.0	21.0	82.1
	Risk Management	52	13.5	13.5	95.6
	Compliance	17	4.4	4.4	100.0
	Total	385	100.0	100.0	

Type of Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Private Bank	110	28.6	28.6	28.6
	Government Bank	110	28.6	28.6	57.1
	Joint Venture Bank	165	42.9	42.9	100.0
	Total	385	100.0	100.0	

Have you received any specific training on cybersecurity?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	279	72.5	72.5	72.5
	No	106	27.5	27.5	100.0
	Total	385	100.0	100.0	

On a scale of 1 to 5, how would you rate your level of familiarity with financial technology (FinTech)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very Low	2	0.5	0.5	0.5
	Low	25	6.5	6.5	7.0
	Neutral	113	29.4	29.4	36.4
	High	219	56.9	56.9	93.2
	Very High	26	6.8	6.8	100.0
	Total	385	100.0	100.0	

How would you rate the overall preparedness of your bank against cybersecurity threats specific to the banking sector in Nepal?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very prepared	58	15.1	15.1	15.1
	Prepared	219	56.9	56.9	71.9
	Neutral	86	22.3	22.3	94.3
	Unprepared	22	5.7	5.7	100.0
	Total	385	100.0	100.0	

What is the frequency of cybersecurity training provided to employees in your

bank?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Monthly	84	21.8	21.8	21.8
	Quarterly	181	47.0	47.0	68.8
	Bi-annually	100	26.0	26.0	94.8
	Annually	20	5.2	5.2	100.0
	Total	385	100.0	100.0	

Has your bank implemented any of the following Nepal-specific cybersecurity guidelines or frameworks?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Guidelines issued by Nepal Rastra Bank (NRB)	139	36.1	36.1	36.1
	Local industry best practices	146	37.9	37.9	74.0
	International standards	74	19.2	19.2	93.2
	None of the above	26	6.8	6.8	100.0
	Total	385	100.0	100.0	

What are the most common types of cybersecurity incidents your bank has faced in the last year?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unauthorized access attempts	108	28.1	28.1	28.1
	Phishing attacks targeting Nepali customers	194	50.4	50.4	78.4
	Fraudulent transactions	42	10.9	10.9	89.4
	Data breaches involving customer information	41	10.6	10.6	100.0
	Total	385	100.0	100.0	

How does your bank ensure compliance with cybersecurity regulations set forth by Nepal Rastra Bank (NRB)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Regular audits and compliance checks	116	30.1	30.1	30.1
	Implementation of NRB-mandated security measures	199	51.7	51.7	81.8
	Staff training and awareness programs	29	7.5	7.5	89.4

	Third-party security assessments	41	10.6	10.6	100.0
	Total	385	100.0	100.0	

Appendix III: Descriptive Statistics

Descriptive Statistics

	N	Mean	Std. Deviation
I feel confident in my ability to identify cyber threats and vulnerabilities.	385	3.6494	0.69158
I believe I have the necessary skills to respond effectively to cyber attacks.	385	3.6545	0.69420
I am confident in my ability to implement cybersecurity measures effectively.	385	3.6623	0.69990
I feel empowered to take proactive measures to enhance cybersecurity in my bank.	385	3.6571	0.68985
I believe my actions contribute significantly to improving cybersecurity in my bank.	385	3.6675	0.68739
I am confident in my ability to communicate cybersecurity risks effectively to colleagues and stakeholders.	385	3.6753	0.69300
I believe that my proactive approach to cybersecurity contributes positively to the overall security posture of my bank.	385	3.6701	0.69430
I am aware of the importance of protecting sensitive information in my bank.	385	3.9143	0.55942
I adhere to security policies and procedures to safeguard confidential data.	385	3.9870	0.50759
I regularly update my knowledge on information security best practices.	385	4.0000	0.50518
I am vigilant about potential security threats and risks in my work environment.	385	3.8987	0.55210
I take proactive measures to prevent data breaches and unauthorized access to information.	385	3.7792	0.61710
I understand the potential consequences of data breaches and unauthorized access to sensitive information in my bank.	385	3.8130	0.58749
I actively participate in information security training programs to enhance my knowledge and skills in safeguarding data.	385	3.8701	0.56252
There is a culture of embracing technology advancements in my bank.	385	3.9091	0.42025
Employees are encouraged to adopt and adapt to new technologies in their work.	385	3.9065	0.42277
There are opportunities for continuous learning and training on technological tools and systems.	385	3.8961	0.42648

Technology is viewed as a strategic asset that enhances banking effectiveness.	385	3.9039	0.42526
Innovation and creativity are valued and promoted within the technological landscape of the bank.	385	3.8779	0.43679
Technology-driven innovation is encouraged and supported by leadership within my bank.	385	3.8831	0.44412
There is a culture of collaboration and knowledge sharing regarding technological advancements and their implications for cybersecurity.	385	3.8753	0.45074
I possess the necessary technical skills to effectively manage cybersecurity systems.	385	3.7117	0.59292
I receive adequate training and support to enhance my cybersecurity competencies.	385	3.7377	0.59184
My bank invests in developing the skills of its employees in cybersecurity.	385	3.7558	0.56146
I feel confident in my ability to troubleshoot and resolve cybersecurity issues.	385	3.6987	0.60175
I continuously seek opportunities to improve my cybersecurity knowledge and skills.	385	3.7740	0.57586
I am proficient in using cybersecurity tools and technologies to mitigate risks effectively.	385	3.6597	0.64231
Continuous professional development opportunities are provided to enhance employees' cybersecurity competencies and skills.	385	3.7299	0.55880
My bank prioritizes cybersecurity as a fundamental aspect of its operations.	385	3.9792	0.39474
There are robust cybersecurity measures in place to protect sensitive information.	385	4.0234	0.44132
I feel confident in the cybersecurity measures implemented by my bank.	385	3.9896	0.39515
Cybersecurity is integrated into the overall business strategy of my bank.	385	3.9714	0.39093
My bank regularly evaluates and updates its cybersecurity protocols to address emerging threats.	385	3.9766	0.39128
My bank has established clear policies and procedures for incident response and breach management.	385	3.9740	0.39443
I feel assured that my bank prioritizes cybersecurity investments to stay ahead of evolving threats and vulnerabilities.	385	3.9688	0.38060
SEF	385	3.6623	0.68361
INS	385	3.8945	0.49688
TEC	385	3.8931	0.41308
CAS	385	3.7239	0.56131
CYS	385	3.9832	0.38110
Valid N (listwise)	385		

Appendix IV: Correlation Analysis

Correlations

		SEF	INS	TEC	CAS	CYS
SEF	Pearson Correlation	1	.826**	.628**	.905**	.543**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000
	N	385	385	385	385	385
INS	Pearson Correlation	.826**	1	.744**	.813**	.648**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000
	N	385	385	385	385	385
TEC	Pearson Correlation	.628**	.744**	1	.702**	.742**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000
	N	385	385	385	385	385
CAS	Pearson Correlation	.905**	.813**	.702**	1	.584**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000
	N	385	385	385	385	385
CYS	Pearson Correlation	.543**	.648**	.742**	.584**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	
	N	385	385	385	385	385

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix V: Regression Analysis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.756[a]	0.571	0.567	0.25082

a. Predictors: (Constant), CAS, TEC, INS, SEF

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.867	4	7.967	126.639	.000[b]
	Residual	23.905	380	0.063		
	Total	55.772	384			

a. Dependent Variable: CYS

b. Predictors: (Constant), CAS, TEC, INS, SEF

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.

		B	Std. Error	Beta		
1	(Constant)	1.248	0.126		9.904	0.000
	SEF	0.343	0.048	0.006	-0.071	0.009
	INS	0.166	0.053	0.217	3.109	0.002
	TEC	0.536	0.049	0.581	10.947	0.000
	CAS	0.373	0.059	0.005	0.064	0.009

FINANCIAL TECHNOLOGY AND CYBERSECURITY IN COMME...

By: Susma Khatiwada

As of: Jul 3, 2024 2:43:28 PM
21,769 words - 17 matches - 2 sources

Similarity Index

1%

Mode: Summary Report

sources:

142 words / 1% - from 28-May-2024 12:00AM
ir.knust.edu.gh

130 words / 1% - from 04-May-2023 12:00AM
www.researchgate.net

paper text:

ABSTRACT This study evaluates the impact of financial technology (Fintech) on cybersecurity in commercial banks in Nepal, aiming to address the challenges posed by the digitization of financial services. By analyzing the relationship between Fintech adoption and cybersecurity measures, the study seeks to identify potential risks and vulnerabilities while assessing the overall impact of financial technology on commercial banks in Nepal. The research design encompasses a descriptive and causal-comparative approach, targeting employees in commercial banks within the Kathmandu Valley, Nepal. A sample size of 385 participants is selected using convenience sampling, drawn from various types of banks. Data collection is conducted through structured questionnaire surveys to capture relevant variables and factors identified in the literature, employing a five-point Likert scale for measurement. Statistical software such as Microsoft Excel and SPSS are utilized for data analysis, employing descriptive statistics, correlation analysis, and multivariate regression models. These analytical tools allow for the exploration of the relationship between Fintech adoption and cybersecurity measures, controlling for other relevant factors outlined in the research framework. The findings reveal that independent variables such as self-efficacy, information security, technological culture, and competence and skill collectively serve as significant determinants of cybersecurity readiness in commercial banks in Nepal. The regression analysis indicates a positive impact of each independent variable on cybersecurity, emphasizing the importance of organizational culture and employee empowerment in addressing cybersecurity challenges effectively. Practically, the study underscores the importance of enhancing cybersecurity measures in commercial banks, especially in light of increasing Fintech adoption. Theoretical implications contribute to understanding the complex dynamics between Fintech and cybersecurity readiness. Recommendations include implementing robust cybersecurity protocols, fostering a culture of cybersecurity awareness, and investing in continuous training and education for employees to mitigate cyber threats effectively. Keywords: Financial technology, cybersecurity, Fintech adoption, Self-efficacy, Information security ii CHAPTER I INTRODUCTION 1.1 Background of the Study Financial technology, commonly known as Fintech, represents a transformative force in the financial services industry, leveraging technology to enhance operations and accessibility (Alodhiani et al., 2023). This innovation has led to the emergence of cellular banks, mobile investing services, and digital currencies like Bitcoin, revolutionizing how financial services are delivered and accessed globally. Start-ups, incumbent banks, and IT firms collaborate within the Fintech sector to improve or replace traditional financial services, driving efficiency and expanding market reach (Stanciu & Tinca, 2017). As Peters et al., (2015) note, modern financial institutions increasingly adopt Fintech solutions to advance service offerings and bolster market competitiveness. This trend underscores the pivotal role of technology in reshaping financial landscapes and driving economic growth. However, alongside its benefits, the proliferation of Fintech introduces new