Effects of Cybercrime in E-banking Systems

Siham Amna Muawia Shaddad

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Science
in
Banking and Finance

Eastern Mediterranean University
February 2023
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Ali Hakan Ulusoy
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Banking and Finance.

Prof. Dr. Nesrin Özataç
Chair, Department of Banking and Finance

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Banking and Finance.

Prof. Dr. Salih Katırcıoğlu
Supervisor

Examining Committee

1. Prof. Dr. Salih Katırcıoğlu

2. Asst. Prof. Dr. Barış Memduh Eren

3. Asst. Prof. Dr. Nigar Taşpınar

ABSTRACT

Cybercrime has become a significant threat to the e-banking industry, causing devastating consequences for financial institutions, customers, and regulatory authorities. This paper examines the effects of cybercrime in e-banking systems and the measures that can be taken to prevent such attacks.

The effects of cybercrime on e-banking systems can be devastating, including financial losses, reputational damage, legal liability, and loss of customer trust. This can cause significant reputational damage to financial institutions, resulting in a loss of business and potential legal liability. Moreover, cybercrime in e-banking systems can result in operational disruptions, causing significant financial and reputational harm to financial institutions. Cybercriminals can use ransomware attacks to encrypt critical data, demanding a ransom payment in exchange for releasing it. Such attacks can cripple e-banking systems, causing significant disruption to the institution's operations and leading to a loss of customer trust.

To prevent cybercrime in e-banking systems, financial institutions must implement robust cybersecurity measures. This includes strong authentication protocols, encryption, regular security assessments, and training for employees and customers on safe e-banking practices. By taking proactive measures to prevent cybercrime, e-banking systems can ensure the security and integrity of their financial data and maintain customer trust.

Keywords: cybercrime, e-banking, cybersecurity

ÖZ

Siber suç, e-bankacılık sektörü için önemli bir tehdit haline geldi ve finansal kurumlar, müşteriler ve düzenleyici makamlar için yıkıcı sonuçlara neden oldu. Bu makale, e-bankacılık sistemlerinde siber suçların etkilerini ve bu tür saldırıları önlemek için alınabilecek önlemleri incelemektedir.

Siber suçun e-bankacılık sistemleri üzerindeki etkileri, mali kayıplar, itibar zedelenmesi, yasal sorumluluk ve müşteri güveni kaybı dahil olmak üzere yıkıcı olabilir. Bu, finansal kurumlarda önemli itibar zedelenmesine yol açarak iş kaybına ve potansiyel yasal sorumluluğa neden olabilir. Ayrıca, e-bankacılık sistemlerindeki siber suçlar, operasyonel aksamalara yol açarak finansal kurumlara önemli mali ve itibari zararlar verebilir. Siber suçlular, kritik verileri şifrelemek için fidye yazılımı saldırılarını kullanabilir ve bunları serbest bırakma karşılığında bir fidye ödemesi talep edebilir. Bu tür saldırılar e-bankacılık sistemlerini çökertebilir, kurumun operasyonlarında önemli aksamalara neden olabilir ve müşteri güvenini kaybetmesine yol açabilir.

E-bankacılık sistemlerinde siber suçları önlemek için finans kuruluşlarının sağlam siber güvenlik önlemleri alması gerekiyor. Buna güçlü kimlik doğrulama protokolleri, şifreleme, düzenli güvenlik değerlendirmeleri ve güvenli e-bankacılık uygulamaları konusunda çalışanlar ve müşteriler için eğitim dahildir. E-bankacılık sistemleri, siber suçları önlemek için proaktif önlemler alarak finansal verilerinin güvenliğini ve bütünlüğünü sağlayabilir ve müşteri güvenini koruyabilir.

Anahtar Kelimeler: siber suç, e-bankacılık, siber güvenlik

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 What is E-Banking?

1.1.1 Definition of E-Banking

E-banking, also known as electronic banking, is the use of electronic means to conduct financial transactions and gain access to banking services (Boyd, 2010). It has a long history, beginning with the launch of the first online banking service in the United Kingdom in 1983. (Smith, 2019). Customers benefit from e-banking in a variety of ways, including convenience, speed, and increased accessibility (Freedman, 2017). E-banking adoption has increased significantly in recent years, with the global e-banking market expected to reach $4.72 trillion by 2023. (Zhang et al., 2020). This expansion has had a significant impact on the global economy, with e-banking widely regarded as a driver of financial inclusion and development (World Bank, 2018). However, the increased use of e-banking exposes individuals and organizations to new types of cybercrime, such as phishing attacks and financial fraud (Hollingsworth & Brickey, 2018). Understanding the effects of cybercrime in e-banking systems is critical for developing effective strategies to mitigate these risks and ensure e-continued banking's growth and stability.

1.1.2 History of E-Banking

The concept of e-banking dates back to 1983, when the Royal Bank of Scotland launched the first online banking service in the United Kingdom (Smith, 2019). Since then, e-banking has evolved rapidly and has become an essential component of the

financial industry. The development of mobile banking and the widespread adoption of smartphones and tablets in the early 2000s increased the accessibility and convenience of e-banking for customers (Chang, 2016). E-banking is now used for a wide range of financial transactions, such as account management, bill payment, money transfer, and investment management (Boyd, 2010). While e-banking has provided significant benefits to consumers and financial institutions, it has also introduced new challenges and risks, such as cybercrime and concerns about data privacy (Hollingsworth & Brickey, 2018). Understanding the evolution of e-banking and its impact on the financial industry is critical in addressing these issues and ensuring e-continued banking's growth and stability.

1.1.3 Current State of E-Banking

Consumers and businesses all over the world use e-banking, which has become an integral part of the financial industry. According to a World Bank report, 54% of adults in developing countries and 89% in developed countries used e-banking services in 2019. (World Bank, 2020). This trend is set to continue, with the global e-banking market expected to reach $8.3 trillion by 2024. (Allied Market Research, 2019).

Customers have embraced the convenience and accessibility of the e-banking services it provides. Customers who use e-banking can conduct financial transactions at any time and from any location, eliminating the need to visit a physical bank branch (Boyd, 2010). This has benefited individuals and businesses in remote areas or with limited access to traditional banking services in particular (Chang, 2016). Furthermore, e-banking has introduced new features such as budgeting tools and financial planning services that have assisted customers in better managing their finances (Smith, 2019).

E-banking has also benefited financial institutions significantly. It has decreased the cost of traditional banking services while increasing operational efficiency (Hollingsworth & Brickey, 2018). Furthermore, e-banking has created new revenue streams for financial institutions, such as online sales of financial products and services (Boyd, 2010). However, as e-banking has grown in popularity, so have the risks and challenges. Cybersecurity threats, data privacy concerns, and regulatory compliance are just a few of the issues confronting the e-banking industry (World Bank, 2020).

Addressing these issues is critical to the continued growth and stability of e-banking. According to a World Bank report, the percentage of adults with a financial institution or mobile money account increased from 62% in 2014 to 69% in 2017 (Kunt et al.,2017). This rise is due to the widespread adoption of digital financial services, such as e-banking, in both developed and developing countries. E-banking has become so popular that it is expected to overtake traditional banking methods soon (Iqbal et al., 2020). Despite its ease of use and widespread adoption, e-banking is not without its challenges. The risk of cybercrime, which can have serious consequences for individuals and financial institutions, is one of the main concerns. In the following sections, we will look at how cybercrime affects e-banking systems and what steps are being taken to mitigate these risks.

1.1.4 E-Banking and the Global Economy

E-banking has had a significant impact on the global economy, especially in the development and expansion of financial systems and markets. The ability to conduct financial transactions electronically has increased the speed and efficiency of financial operations, which has resulted in an increase in international trade and investment (Andrade & Bagnall, 2013). E-banking has also contributed to the democratization of

financial services by allowing individuals and small businesses in underserved or remote areas to access previously unavailable financial products and services (Majid, 2017).

Furthermore, e-banking played a role in the late-2000s global financial crisis. The use of complex financial instruments, such as mortgage-backed securities, made possible by e-banking systems has been identified as a factor contributing to the crisis (Jeon, 2012). This demonstrates the significance of effective regulation and risk management in the e-banking industry, particularly in the context of global financial systems.

Overall, the global economy has been significantly impacted by the adoption and development of e-banking, both in terms of the benefits and challenges it brings. As e-banking evolves, financial institutions and policymakers must consider the economic implications and take appropriate measures to mitigate risks while maximizing benefits.

1.2 Thesis Statement

E-banking has transformed the way financial transactions are conducted, providing customers with convenience and accessibility while increasing efficiencies for financial institutions. However, the increased reliance on electronic systems has made e-banking vulnerable to various types of cybercrime, such as phishing attacks, malware, and data breaches. The purpose of this literature review is to investigate the effects of cybercrime on e-banking systems and to provide insight into the measures that can be implemented to mitigate these risks. This research aims to provide a comprehensive understanding of the impact of cybercrime on e-banking by reviewing available data and studies on the subject, as well as recommendations for improving

cybersecurity in the industry, by reviewing available data and studies on the subject.

1.3 Aim and Contribution

The purpose of this article is to assess the impact of cybercrime on e-banking and to provide methods to limit the risks. The significance of minimizing the risks connected with e-banking cannot be emphasized, given that it accounts for a sizable share of the financial industry. As a result, this paper will examine the consequences of cybercrime on e-banking, counter-cybercrime measures, and viable ways to lessen cybercrime's influence on e-banking. Furthermore, by analyzing previous studies and research, this paper will provide documentation of the effectiveness of these countermeasures. It is anticipated that by doing so, companies and organizations would be able to defend themselves from cybercrime while still maintaining the security of their e-banking services.

Chapter 2

LITERATURE REVIEW

2.1 The Three Levels of E Banking Services

Level 1: The entry level position that institutions advertise on their platforms. The banks are providing information to consumers about its own commodities via this medium. Additionally, some financial institutions might accept and answer questions by email.

Level 2: Customers can easily find their financial accounts, publish directions, or bundles for additional features, as well as more. Financial institutions, on either side, prohibit its clients from making investments transactions related to existing loans.

Level 3: In the third degree, institutions permit their clients to utilize the funds that they owe them to make modifications to personal spending plans, send invoices, even buy, or sell commodities.

E banking is an unique way to get resources from the majority of banking institutions. In addition, a lot of modern banks offer financial services through electronic or on demand commerce platforms. Additionally, many institutions that don't have a substantial form in the US are "net most effective."

2.2 Two Types of E-banking

Informational Websites: These websites provide general statistics on financial institutions and their services and products to customers.

Transactional Websites: These websites permit clients to conduct transactions on the bank's internet site. Further, those transactions can vary from a straightforward retail account stability inquiry to a sizeable enterprise-to-commercial enterprise funds switch. The following table lists a few standard retail and wholesale e-banking offerings by banks and financial establishments.

2.3 Importance of E-banking

In this section, there will be a discussion of the importance of e-banking based on businesses, individual customers, and banks.

This paragraph will discuss the importance of E-banking based on banks perspective:

- Cheaper transactions-electronic transactions are the cheapest.
- Human error is reduced because information is transmitted electronically, leaving no room for human error.
- Reduced paperwork-electronic files reduce paperwork and streamline the process. It is also environmentally friendly.
- Lower fixed expenses — because there is less need for branches, the set price is lower.
- More loyal customers - Because e-banking services are simple to use, banks enjoy high levels of customer satisfaction.

This paragraph will discuss the importance of E-banking based on customers' perspective:

- Customer convenience — customers can access their accounts and conduct transactions at any time, 24 hours a day, seven days a week, 365 days (approximately 12 months) a year.
- Lower transaction fees — by not having to visit the branch for each transaction, the

client saves both time and money.

- There are no geographical boundaries — in previous monetary systems, distances could impede certain banking operations. Geographical barriers, on the other hand.

This paragraph will discuss the importance of E-banking based on business perspective:

- Account audits - Entrepreneurs and authorized staff members can quickly examine various accounts using an internet banking platform. This allows administrators to monitor account activity while also ensuring the overall stability of the user's account.
- Increased Productivity - Electronic banking increases productivity. It allows for the processing of recurring monthly transactions as well as additional capabilities that increase the company's efficiency.
- Cost reduction - Most banking arrangements base costs on the resources used. If a company requires additional assistance with money transfers, deposits, and other services, the bank will charge a higher fee. When users use internet banking, these costs are reduced.
- Errors are reduced - Electronic banking helps to reduce errors in traditional bank transactions. Errors can be costly because of poor handwriting, incorrect information,and other factors. Furthermore, having an easy way to monitor account activity improves the accuracy of financial transactions.
- Reduced fraud – Electronic banking leaves a digital trail for all personnel with the authority to alter banking transactions. As a result, the company understands its operations better, making it more difficult for scammers to wreak havoc.

2.4 Determinants of E-banking Performance

Accessibility:

The accessibility principle (or ease of access) has multiple components. Electronic accessibility, information availability, system dependability, and simplicity of learning the language of usage are the four components of accessibility, according to Rice and Shook (1988). According to Karahanna and Straub (1999), accessibility also includes a third dimension related to interface terminals and platform functioning. According to several investigations, perceived trust is influenced by functioning or a general sense of accessibility (Roy et al., 2001). Similarly, Saeednia and Abdollahi (2012) show how accessibility has a favorable, direct link with security, pointing to various features dependent on a user's opinion of the ease with which digital banking services are available.

Numerous research studies have found that effective knowledge availability results in increased information acquisition and ease of usage (Wyer & Srull, 1986; Lin & Lu, 2000). Additionally, Tan and Teo (2000), Wixom and Todd (2005), and Poon (2008) argue that the exposure of electronic banking assists in the adoption of enhanced technologies and, as a result, its usefulness. Cyr's (2008) notion highlights the need of a navigational software that allows visitors to navigate a website. Applicant accessibility has a major influence on satisfaction since it increases issues highlighted as well as accessibility, raising intents to use e-banking and receive happiness from it. According to Poon (2008), Casalo et al. (2008), and Sadeghi and Hanzaee (2008), accessibility is advantageous for achieving customer satisfaction in the deployment of digital banking (2010).

Lastly, the simplicity of use of electronic banking adds to its usability (Lin & Lu, 2000) since it later specifies user happiness with its usage and efficacy. Thus according Fonchamnyo (2013), the ease of access to online banking influences the potential effectiveness that consumers exhibit toward it, raising the possibility that they would utilize it.

Trust:

Acceptance of online marketplaces necessitates faith in a company's ability to meet its promises while not benefitting from them (Ranaweera et al., 2005). The perception of a lack of trust, especially in digitalization and financial procedures (Gefen, 2000; Pitta et al., 2006). Financial institutions must pay more attention to whether they eliminate user uncertainty and promote good opinions of the firm's actions (Bart et al., 2005). Ganesan (1994).

Past study has discovered that the perceived productivity of e-commerce is influenced by authenticity (Gefen et al., 2003; Shin, 2008). Furthermore, the more consumers trust an online platform, the more likely they are to utilize it, and the less time and sustained attention individuals will commit to examining the platform's characteristics and, indeed, the accessibility of services (Mun oz-Leiva et al., 2012). Previous study has demonstrated that honesty influences efficacy (Yoon, 2009; Sun, 2010; Zhou, 2011).

Trust and contentment are two closely connected notions that have previously been studied. Satisfaction levels are established by a consumer's or customer's belief in a service or product, whether in the online or offline realm (Lin & Wang, 2006). (Chiou, 2004). According to one study (Lee & Chung, 2009; Zhou, 2011), the credibility established by information systems and cellular websites has a favorable and

significant influence on consumer satisfaction and loyalty.

Ease of use:

The individual's assessment of how simple it is to use a particular technology is referred to as ease of use (Davis, 1989; Taylor & Todd, 1995). Furthermore, a literature review on e- transactions revealed that perceived usefulness and ease of use are determined by self-efficacy, so if the purchaser trusts the company's website, the transfer of funds is easier to accomplish, and the purchaser may very well believe that they fully comprehend more and have much less need to manage the situation (Munoz-Leiva, 2008). In terms of perceived trust, Fogg et al. (2002) discovered that perceived ease of use is one of the variables that frequently improve perceived legitimacy, making a website highly trustworthy. Accessibility, according to several researchers, influences perceived trust (Flavian et al., 2006). Thus, ease of use has a negative impact on perceived risks and credibility in the online platform (Featherman & Pavlou, 2003).

In the study of information systems, ease of use has been identified as a factor that influences customer satisfaction (McHaney & Cronan, 1998), as well as a factor that contributes to the implementation of information technologies (Davis, 1989) or e-services (Davis, 1989). Liao and colleagues (1999). Furthermore, Abdinnour-Helm et al. (2005) discovered that ease of use has a direct impact on satisfaction with a commercial company website, whereas Liao and Cheung (2008) hypothesized and statistically evaluated ease of use as a measure of consumers' contentment with internet banking. As a result, in internet banking, ease of use is a predictor of customer loyalty (Yoon, 2010).

Usefulness:

Perceived usefulness is defined as "a prospective customer's subjective belief that implementing a particular technology would improve work efficiency in an institutional context" (Davis et al., 1989, p. 985). According to electronic banking research, they are deploying technologies that allow users to obtain information easily and quickly, which will increase perceived usefulness (Shih & Fang, 2004) as well as contentment (Bhattacherjee & Premkumar, 2004). Numerous studies have found that perceived usefulness has a significant impact on contentment (Zhou & Lu, 2011; Wu, 2013).

2.5 Risks associated with E-banking

Operational Risk:

One of the most frequent types of risk in e-banking is operational risk, often known as transactional risk. It includes the following:

- Improper transaction handling
- Compromises in data security, protection, and confidentiality
- Illegal access towards the bank's information systems
- Agreement non-enforceability.

Aside from technology mistakes, human factors such as incompetence (customers or workers), fraudulent activity, and hackers are potential causes of e-banking operational risk.

Security Risk:

The protection of transactions is critical in financial transactions. All clients expect their transactions to be treated confidentially. Nevertheless, because all knowledge is

accessible online, there will always be the potential that somebody will retrieve it all and exploit it. Cyber risks and security breaches to the institution's facilities also pose a security risk to e-banking.

System Architecture and Design:

Financial institutions must have suitable system designs and regulations to address the operational and security risks associated with e-banking. Financial institutions are always at risk of selecting the wrong architecture of the system and technologies and having insufficient regulatory mechanisms. If the bank has an antiquated system that cannot be upgraded, it may result in investment loss and inadequate management. In order to eliminate system vulnerabilities, banks must constantly update existing systems to stay up with fast-evolving technologies. Additionally, the institution's employees must be trained regularly to keep up with emerging technology.

Reputation risk:

The reputation of a business is critical to its success. Financial institutions run the danger of losing their reputation when it comes to electronic banking if they don't maintain key operations or satisfy client expectations. As a result, funding is reduced, or clients are lost. A few factors that contribute to this hazard include:

- systems or products that don't function as expected.
- structural flaws
- unauthorized access (external or internal)
- consumer misinformation on the rules and procedures of utilizing e-banking.
- problems with communication that prohibit customers from attempting to enter their accounts.

Legal Risk:

If any of the participants who took part in the transactions violate any laws, rules, or established guidelines, or whether the fundamental rights and obligations of any of the parties are not recognized, then there is a legal responsibility. Since the e-banking sector is expanding, there needs to be additional clarity and uniformity on important rules and standards. As a result, the regulatory risk increases.

Money laundering risk:

Any transactions made through the e-banking gateway are done so virtually. As a result, institutions must use conventional methods to detect and stop illegal conduct. Even though there are laws against financial fraud, it is questionable whether they apply to wire transfers. Institutions consequently run the danger of financial crime.

Cross-border risk:

The underlying concept behind electronic banking is to increase the distribution network of both customers and businesses. This suggests that the proliferation might transcend international borders. It generates a number of international risks:

Legal and regulatory issues: There is a chance that legislative norms in particular countries and regulatory differences between different national bodies will be unclear.

Operational risk: Operations and maintenance risk arises if somehow the bank uses an internet service company in another country because it is difficult to monitor. Credit risk may increase with international transactions. This would be because it is challenging to examine a credit application from a customer in a different country.

Strategic Risk:

This is the current and future risk to revenue growth brought on by subpar financial decision or subpar risk management, and it pertains to the following issues:

- Creating a business proposal
- Obtaining enough funds to execute the corporate plan.
- In the case of external suppliers, the vendor's trustworthiness is critical.
- Each alteration in the workplace environment is a source of concern for personnel.
- It is the level of technologies used by current technologies, and so on.

2.6 The Rise of E-banking

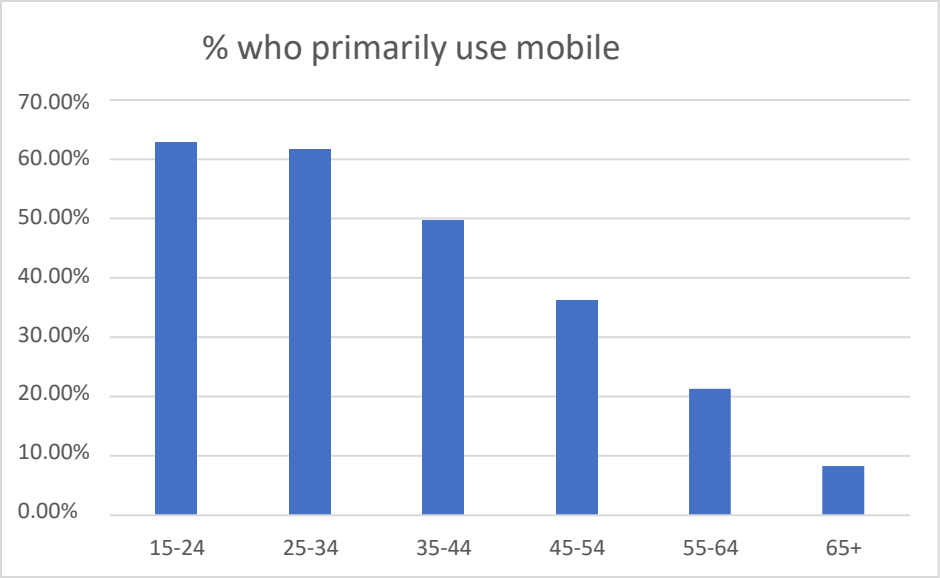
2.6.1 Mobile and Online Banking Usage

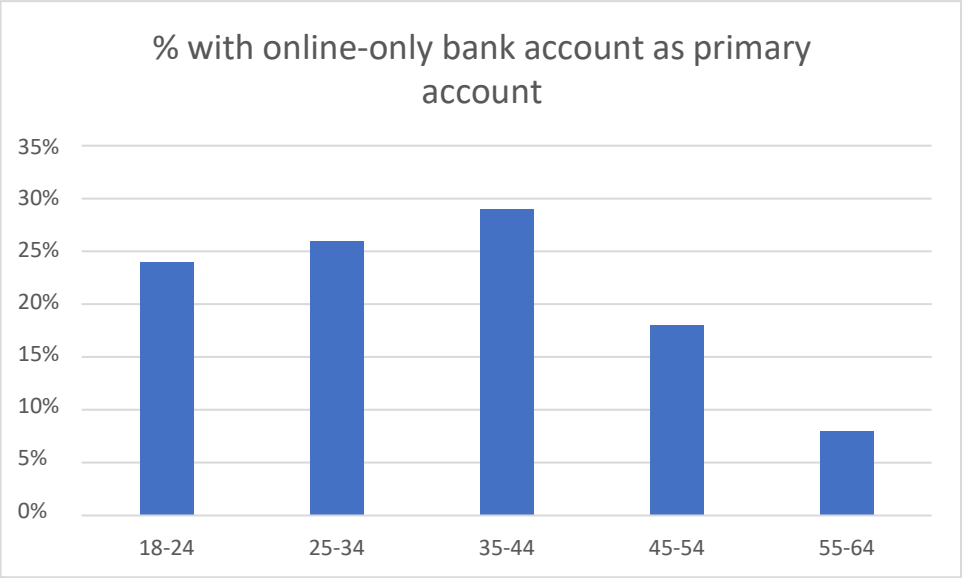
Mobile and online banking have grown in popularity in recent years due to the convenience and accessibility they provide consumers. According to Bennett and Bennett (2022), the number of people using mobile banking apps increased by 24.9% between 2015 and 2019. This trend is most likely due to the widespread use of smartphones, as well as the various features and benefits provided by mobile banking apps, such as the ability to check account balances, transfer funds, and pay bills from anywhere at any time.

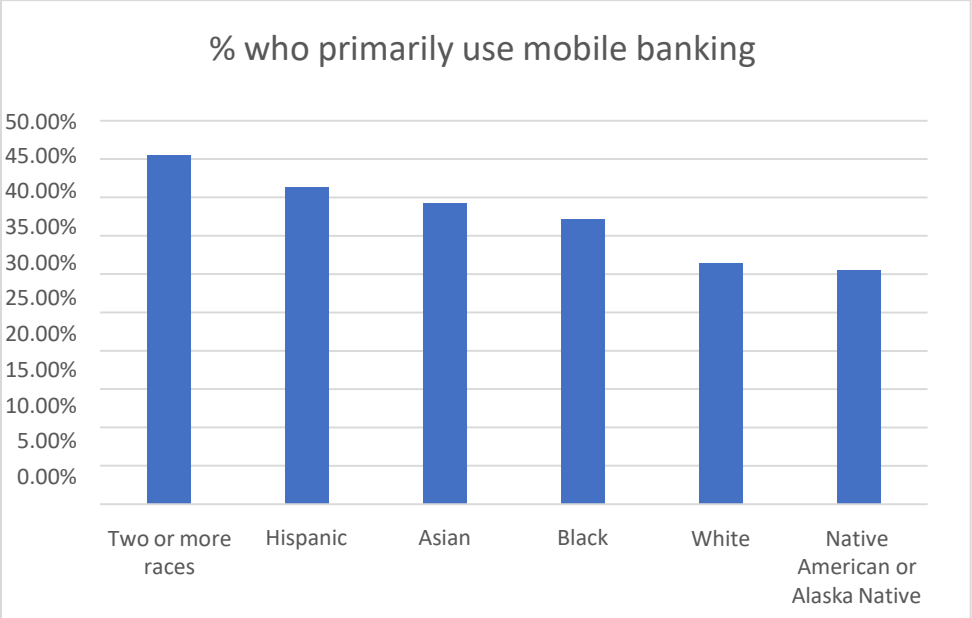
The 1st chart with the title "% who primarily uses the mobile banking" shows the percentage of people in various age groups who primarily use mobile banking, according to data from https://www.bankrate.com/. According to thedata, younger age groups are more likely to use mobile banking, with 62.9% of those aged 15-24 and 61.7% of those aged 25-34 doing so primarily. The percentage decreases with age, with only 8.3% of those 65 and older primarily using mobile banking.

The 2nd chart with the title "% with online-only bank account as primary account" depicts the proportion of people in various age groups who have an online- only bank account as their primary account. According to the data, younger age groups are more likely to have an online-only bank account as their primary account, with 24% of those aged 18-24 and 26% of those aged 25-34 having such an account. Withonly 8% of those aged 55-64 having an online-only bank account as their primary account, the percentage decreases with age.

The 3rd chart with the title "% who primarily uses mobile banking" depicts the proportion of people of various races/ethnicities who primarily use mobile banking. People of two or more races and Hispanics are the most likely touse mobile banking, according to the data, with 45.5% and 41.3%, respectively. With39.3% and 37.2%, Asian and Black people are also relatively likely to use mobile banking. With 31.4% and 30.5%, respectively, white people and Native Americans or Alaska Natives are the least likely to use mobile banking.







Finally, data show that younger age groups and people of specific races/ethnicities are more likely to use mobile banking and have online-only bank accounts as their primary accounts. Various factors, such as technological proficiency and access to mobile banking services, may influence these trends. More research may be required to fully understand the factors contributing to these trends. Financial institutions must be aware

of these trends in order to effectively serve and accommodate their customers' needs. Overall, the data indicates that mobile and online-only banking are becoming more popular, especially among younger age groups and certain races/ethnicities.

2.6.2 E-banking Adoption Rate

Global e-banking adoption rates have risen as consumers increasingly turn to digital platforms for financial services. Digital banking's convenience and accessibility have made it an appealing option for many, particularly in areas where traditional brick-and-mortar branches may be scarce. Regulators, who have implemented new frameworks and granted licenses to digital banking operators to encourage the growth of this sector, have also backed this shift.

According to a recent report by Finder, a financial comparison platform based in Singapore, digital banking adoption is currently leading the way, with 32% and 24.9% of adults having a digital bank account, respectively. However, the report predicts that by 2026, 28% of people globally will have a digital bank account, up from 17% in 2021. This expansion is expected to be fueled in part by increased internet coverage in countries such as Vietnam, Indonesia, Malaysia, and the Philippines. 2021 (Kr-Asia.com).

The report examined gender differences in digital banking usage in addition toadoption rates. While men were found to be more likely to have a digital bank accountin 19 of the 30 countries surveyed, the gap was especially pronounced in countries such as the UAE, Brazil, Finland, and Japan, where the difference reached 8%. Women, on the other hand, were found to be more likely to have a digital bank accountin Singapore and Vietnam, with a 1% gender gap.

Overall, banking adoption is increasing and is expected to continue to rise in the coming years. As digital technologies continue to disrupt the traditional banking industry, financial institutions must adapt and meet their customers' changing needs.

2.6.3 Trends in Digital Payments

Over the last few years, digital payment trends have continued to evolve, with U.S. consumers increasingly using various digital payment options. Almost nine out of ten Americans now use some form of digital payment, according to McKinsey's 2022 Digital Payments Consumer Survey. The use of multiple forms of digital payment has also increased significantly, with 62% of respondents indicating that they use two or more. In-app and peer-to-peer (P2P) purchases have grown the most, adding to the already widespread use of online payments, which 69% of consumers use. Consumers expect to have a digital wallet within the next two years, with a significant increase in the number of consumers planning to use three or more digital wallets in the coming years, rising from 18% in 2021 to 30% in 2022. This trend represents a significant departure from the traditional model of carrying a single leather wallet (Anan et al., 2022). When asked who their preferred provider for digital wallets was, consumers of all ages overwhelmingly chose their bank, with smartphone manufacturers and tech companies coming in second. Consumers are more likely to use digital wallets from providers such as PayPal, Apple Pay, and Google Pay in practice.

Consumers consistently seek payment functionality, the integration of loyalty and rewards capabilities, solutions that offer a broad range of financial services, and compatibility with existing apps when choosing a wallet. Furthermore, when selecting a digital wallet, consumers prioritize security and privacy. Anan et al. (2022) report that the popularity of buy now, pay later (BNPL) financing has also increased

significantly, with 28% of respondents reporting using BNPL options in the previous year. This trend is especially prevalent among younger consumers, with 44% of those aged 18-24 using BNPL options. BNPL options are popular among consumers, particularly those who do not have access to traditional credit options, due to their convenience and flexibility. In addition, cryptocurrency has gained popularity in recent years, with 10% of respondents reporting use of cryptocurrency in the previous year.

This trend is even more prevalent among younger consumers, with 20% of those aged 18-24 using cryptocurrency. Cryptocurrency's perceived benefits, such as decentralization and anonymity, make it an appealing option for some consumers.

However, many consumers are concerned about the lack of regulation and the volatile nature of cryptocurrency prices. As consumers seek convenience, flexibility, and security in their financial transactions,digital payment trends continue to evolve. To remain competitive in the digitalpayments space, providers must consider these trends as well as changing consumer preferences because digital payment options are frequently provided through online banking platforms, the growing use of digital payments is closely related to the growth of e- banking. Consumers can conduct financial transactions and access banking services online rather than visiting a physical branch.

This ease of use has resulted in widespread adoption of e-banking, with many consumers relying primarily on online platforms for their banking needs. Digital payment options, such as digital wallets and BNPL financing, are frequently integrated with e-banking platforms, making these services more accessible and usable for consumers. Integrating digital payment optionswith e-banking platforms also provides

consumers with a more seamless experience by allowing them to access and manage their financial transactions in one location. E-banking will most likely see increased adoption as the use of digital payment options grows.

2.6.4 E-Banking Infrastructure

The growth of e-banking infrastructure has had a significant impact on the banking industry especially in developing countries. E-banking enables banks to reach a larger customer base and provide a wider range of services than traditional brick-and-mortar branches. Customers can also access their accounts and conduct transactions from any location with an internet connection, making banking more convenient and efficient.

However, implementing e-banking infrastructure necessitates significant bank investments and infrastructure changes. It also raises new security concerns, as online financial transactions are vulnerable to cyber-attacks. Banks must ensure that their e-banking infrastructure is secure and compliant with regulations to mitigate these risks.

Evidence suggests that expanding e-banking channels can boost a bank's market share. According to (Nazaritehrani & Mashali, 2020), internet banking, point of sale, and telephone banking all had a positive impact on market share. In contrast, the development of mobile banking and automated teller machines had no significant impact. This suggests that banks can increase their market share by investing in and developing innovative e-banking channels that meet their customers' needs and preferences.

The infrastructure of e-banking is constantly evolving, with new technologies and services being developed and introduced. Mobile banking apps and digital wallets, for example, have grown in popularity in recent years. As a result, banks must constantly

assess and improve their e-banking offerings to stay current with the latest developments in e-banking infrastructure.

Overall, the development of e-banking infrastructure has had a significant impact on the banking industry, both in terms of customer convenience and efficiency, as well as the competitive advantage it can provide banks. As such, it is an important research topic for financial researchers and practitioners.

2.7 What is Cybercrime?

Cybercrime is the use of computers as weapons to further criminal goals such as fraud, child pornography, intellectual property trafficking, personal information theft, and privacy invasion. As computers become more important in business, entertainment, and government, cybercrime is becoming more serious, particularly on the Internet because computers and the Internet were widely used in the United States at the time, the majority of the early victims and perpetrators of cybercrime were Americans.

However, in the twenty-first century, only a few countries are immune to cybercrime. The majority of cybercrimes target personal, corporate, or government information. Cyber-attacks do not target physical beings, but rather an individual's identity or an organization's digital body. This is a set of data characteristics used to identify individuals and organizations on the Internet. In other words, our virtual I.D.s are an essential part of our daily lives in the digital age. We are a collection of numbers and identifiers stored in various government and commercial computer databases. Cybercrime highlights the significance of networked computers in our lives as well as the vulnerability of irreversible facts such as personal identities.

2.8 Types of Cybercrime

Cybercrime manifests itself in a multitude of ways. The majority of cybercrimes are committed with the purpose of earning financial benefit for the offenders, however the techniques by which cybercriminals seek payment might vary. Cases of specific forms of cybercrime include:

Cyber-extortion: An attack or threat of an attack, followed by a monetary supply to put a stop to the activity. Malware attacks are one type of cyber-extortion. The culprit infiltrates a company's networks and encrypts all the company's papers and assets, leaving the data inaccessible until the transaction is completed. This takes the form of a cryptocurrency, such as bitcoin.

Crypto jacking: An exploit that employs software to mine Cryptocurrency without the individual's consent through browsers. Crypto-jacking assaults may entail the victim's computer being infected with crypto-mining programs. Nevertheless, if the user's browser has a tab or window active on the rogue domain, most assaults rely on JavaScript code which performs in-browser extraction. There is no need to download ransomware because the in-browser extraction script is compiled when the infected website is loaded.

Identity theft: An assault where a person acquires access to the computer to obtain information about the user. At this point, hackers will use it to steal digital credentials or gain access to critical assets such as banking and credit cards. On the dark net, hackers transact personal data, including banking statements, email, multimedia streams, auction sites, and thus more. Another prevalent type of identity fraud is individual medical records.

Credit card fraud: An attack in which hackers gain access to a firm's networks to steal their clients' bank cards and account information. On the dark net, stolen credit and debit cards can be auctioned in bulk, with hacktivists profiting from distributing them to lower-level hackers who earn fraudulent activity against individual accounts.

Cyber-espionage: A cyber-criminal who hacks into a government's and other firms' network systems in exchange for access to personal data. Profits or politics might inspire terrorism. Cyber-espionage operations can include any form of a ransomware attack to assemble, alter, or corrupt information, as well as the usage of network-connected gadgets, such as webcams or closed-circuit television (CCTV) cameras, to spy on targeted individuals or organizations, as well as being able to monitor interactions, such as emails, messages, and online chats.

Software piracy: A cyber-attack involving unauthorized disclosure, dissemination, and usage of software applications for business or personal gain. This sort of Cybercrime is frequently related to copyright encroachments, theft of intellectual property, and patent invasions of privacy.

Exit Scam: Interestingly, the deep web has created a digital counterpart of an old swindle characterized as an exit fraud. Deep web executives shift crypto money stored in global market bank funds towards their wallets in today's version, thus looting from many other felons.

2.8.1 Characteristics of Cybercrime

The basic principle of cybercrime differs significantly from that of traditional crime. In addition, due to the advancement of Internet technology, this crime has received more severe and unrestricted attention than traditional crime. As a result, it is necessary

to investigate the peculiar characteristics of cybercrime. However, some of the most common features of cybercrime include the following:

The first characteristic of cybercrime is its ability to be anonymous. Cybercriminals can use the Internet to hide their identities and locations, making it difficult for law enforcement officials to find them because of this, many cybercriminals operate in the shadows, with few people knowing their true identities or where they are located. This also makes it difficult for victims to report their crimes, as they cannot identify their attackers or locate them on the Internet.

The second characteristic of cybercrime is the geographical challenges; in cyberspace, geographic boundaries are zero. Cybercriminals sitting somewhere in the world quickly commit crimes elsewhere in the world. For example, a Native American-based hacker is hacking a U.S. system.

The third characteristic of cybercrime is the people with specialized knowledge. Cybercrime can only be committed through technology, so one must be proficient on the Internet, computers, and online databases to commit such a crime. People who commit cybercrime are well-educated and have a thorough understanding of how the system functions, making it difficult for law enforcement to apprehend the perpetrators of cybercrime.

The fourth characteristic of cybercrime is its permanence. Cybercriminals often take the essential or valuable information they obtain through their crimes, making it difficult for victims to get that information back. This also makes it difficult for law enforcement officials to investigate and prosecute cybercrimes, as they need to identify and locate many victims to build a case against cyber criminals. As a result, many

cybercriminals operate with impunity, knowing they can operate with negligible risk of being caught.

The last major characteristic is the magnitude of the crime unimaginable; Cybercrime has the potential to cause unimaginable bodily harm and loss of life. Offences such as cyber terrorism and cyber pornography. have a broad reach and can quickly destroy websites and steal company data.

2.9 What Are The Likely Effects Of Cybercrime In General?

Cybercrime has affected individuals, businesses, and governments worldwide, becoming increasingly apparent. From the massive retail heists of 2017 to the WannaCry ransomware attacks of 2017, Cybercrime is causing a significant daily impact. Cybercrime also can affect our nation's infrastructure, such as the 2017 power outage in Georgia.

The long-term effects of Cybercrime are slowly changing the way our society functions. Cybercrime can cause severe economic harm, destroy data, and disrupt services and businesses. A few persistent themes recur as the subject is examined in depth; one of the most visible manifestations of Cybercrime is the illegal use of computers. The National Cyber Security Alliance (NCSA) reports that nearly one-third of all U.S. adults have been victims of Cybercrime at some point. The NCSA also reports that cybercrimes cost American businesses over $45 billion yearly.

2.9.1 How Does Cybercrime Affect Business?

The actual cost of Cybercrime is challenging to ascertain. McAfee published a report on the financial consequences of Cybercrime in 2018, estimating the reasonable yearly cost to the global economy at nearly $600 billion, up from $45 billion in 2014. Since

economic problems can be noticeable as a result of Cybercrime, businesses also can experience severe other catastrophic effects as a result of criminal cyber espionage, including the following:

- Damage to investor perception as a result of a data leak can cause a reduction in a firm's profitability.
- In addition to possible share price reductions, businesses may face higher lending costs and increased complexity in raising financial financing due to a cyberattack.
- The decline of vulnerable client data can result in penalties and punishments for businesses that fail to stop their clients' data. Businesses may also face legal action as a result of the data breach.
- Clients' trust in a corporation and its determination to keep their financial information safe is undermined when its brand identity and reputation are harmed due to a cyberattack. Businesses not only end up losing existing customers after a cyberattack, but they also start losing the potential to obtain fresh clients.
- Businesses may face intense losses due to a criminal cyberattack, such as enhanced insurance premiums, the cost of acquiring cybersecurity firms to handle the incident response and restoration, public relations (P.R.), and many other services about an attack.

2.9.2 How Does Cybercrime Affect The National Defense?

Because cybercrime may endanger public health as well as national security and privacy, it is one of the DOJ's top priorities. The Federal Bureau of Investigation's (FBI) Cyber Division is the agency within the Department of Justice (DOJ) charged with combating cybercrime in the United States.

The Department of HomelandSecurity (DHS) regards cyber-security and perseverance as critical domestic security tasks. Cybercrime is combated by special divisions of organizations such as the UnitedStates Secret Service (USSS) and Immigration and Customs Enforcement (ICE).

The Electronic Crimes Task Force (ECTF) of the United States Secret Service (USSS) investigates cases involving digital types of crime, with a focus on the nation's economic and critical infrastructures. The USSS also runs the National Computer Forensics Institute (NCFI), which provides cyber forensic training to local law enforcement, judges, and district attorneys.

2.9.3 How Does Cybercrime Affect Individuals?

Individually, a cyber-attack can have a wide range of consequences, ranging from the theft of personal data to money extortion or underutilization of data, such as family portraits. Nuclear reactors, healthcare facilities, and financial services firms are all critical infrastructures for society and systems. These systems are, in many ways, just as important as government and corporate systems. The ability to launch large-scale, expensive, and crippling cyber-attacks, including those against critical systems, will only increase the value of such attacks. Criminals will continue to target large organizations with cyber-attacks to further their criminal enterprises.

However, many cyber-attacks are likely to be more disruptive and costly to individuals, such as the Sony Pictures hack, which resulted in the release of millions of personal emails, or the Anthem data breach, which resulted in the exposure of 78 million people's personal information.

2.10 What Has Been Done In The Relevant Literature So Far In The Case Of Cybercrime?

One of the first things to mention is that the existing cybercrime literature needs to be expanded. The first scholarly works on the subject were published in the mid-2000s, and the field has since expanded dramatically. However, the majority of the research to date has focused on Cybercrime as a whole, and more work is needed to investigate the effects of Cybercrime on specific groups.

This is the first major limitation of the literature on the topic, implying that the conclusions about the effects of Cybercrime on specific groups are limited. However, what has been done thus far provides some insight into the types of effects that cybercrime can have on specific groups. For example, one study examined the effects of Cybercrime on people with developmental disabilities (Kline, 2017) and discovered that people with developmental disabilities are significantly more likely than the general population tobecome victims of Cybercrime. Another study looked at the effects of Cybercrime onthe elderly (Braziel & Taylor, 2017) and discovered that elderly people are significantly more likely than younger people to become victims of Cybercrime.

Another study looked at the effects of Cybercrime on small business owners (Domingo, 2017) and discovered that small business owners are significantly more likely than the general population to be victims of Cybercrime. Other studies have looked at the effects of cybercrime on the elderly and the unemployed (Crawley, 2017). (Isac, 2017). Individuals who are otherwise at a higher risk of becoming a victim of Cybercrime are also more likely to become a victim of Cybercrime than thegeneral

population, according to Allison (2017).

Recent events have demonstrated the potential for cyberattacks to have a genuine impact on our lives. Cyberattacks, both successful and unsuccessful, have occurred in a wide range of industries. The goals of these attacks have ranged from causing economic disruption to stealing sensitive data and personal information and using it for financial gain or causing widespread damage to critical infrastructure.

The NotPetya cyberattack was one of the most well-known recent cyberattacks. This attack was launched in June of 2017 with the intention of causing computer damage and economic disruption. The attack took advantage of a vulnerability in the Windows operating system that was discovered and exploited by a malicious actor, infecting millions of computers. The attack was massive in scope, with 80,000 computers in a single Ukrainian government agency infected at one point.

The table below summarizes and analyzes various studies on cybersecurity and topics such as central bank digital currency, foreignness, sustainable development, and more. We hope that by conducting this review, we will gain a better understanding of the various approaches and findings of these studies, as well as how they may inform or impact our current research. By considering the methodologies, conclusions, and implications of these studies, we can gain a more comprehensive understanding of the complex relationship between cybersecurity and these various topics.

Author and year	Topic	Methodology	Conclusions	Implication of current studies
Tian etal., (2022)	Evidence from Global Cyberattacks on Cybersecurity Risks and Central Banks' Attitudes Toward Central Bank Digital Currency	In the context of global cyberattacks, the effects of two categories of cybersecurity threats on central banks' perceptions. CBDC were examined.	Following growing losses from assaults on cryptocurrency assets, central banks' attitudes regarding CBDC changed for the better, but they sharply decreased following more aggressive cyberattacks. Although CBDC introduces systemic risks to national financial systems, it may be able to shield consumers from hazards associated with the private sector.	This study shedslight on how various cybersecurity concerns influence centralbanks' perceptions of CBDC and the possible repercussions forits application inthe financial system.
Masoud and Al-Utaiibi, (2022)	Factors that affect how companies disclose cybersecurityrisk in their financial reports	Examined the linkbetween financial reporting flaws and cybersecurity risk disclosure using a large sample of both penetrated and unbreached US enterprises from 2006 to 2016.	There is a strong and positive correlation between the disclosure of cybersecurity risks and the subsequent reporting of financial inadequacies, indicating that organizations thathave previously disclosed their cybersecurity risks are more likely to encounter financial reporting faults.	According to this study, greater firm-specific cybersecurity risk disclosure may boost audit effort and enhance audit quality. Regulators should think considering pushing businesses to include greater disclosures about cybersecurity risks in their financial reporting.
Ashraf et al., (2022)	Does requiring prompt disclosure of cybersecurity events include trade-offs? Evidence fromdata	Utilizing information from the United States, researchers lookedat how state-level data breach notification rulesaffected the timeand	When under pressure, businesses disclose a data breach 90% faster but 58% less frequently revealthe specifics of the incident. Investors react unfavorably to postponed breach reports, although they	The trade-offs of requiring a disclosure deadline for cybersecurity events are highlighted in this study. When imposing such requirements, regulators shouldtake into account the possible effects on both the timeliness and

	breach disclosure legislation at the state level	specifics of cybersecurity event disclosure.	are understanding of a delay if it allows for the gathering of further breach information.	the specifics of disclosures.
Senarak, (2021)	Cybersecurity expertise and competenciesfor port facility security officers in international seaports: IT and security personnel's perspectives	Conducted a survey of Thailand's international cargoports and examined the findings from the viewpoints of the IT and security staff.	As the port sector becomes increasingly automated and digital, PFSOs will need to havea strong understanding of cybersecurity. They will also oversee managingcyber risk to shield against new cyber threats. To become cybersecurity competent, PFSOs should learn to integraterisk managementwith cyber risk management and cybersecurity understanding.	To appropriately protect digital port facilities from emerging cyberthreats, this study underlines the need for PFSOs to increase their cybersecurity knowledge. Port security guards may consider participating in educational and training courses to get these skills.
Rodrigues et al., (2022)	A multi-stakeholder cognition-driven framework for artificial intelligence, digital transformation, and cybersecurity in the banking industry	Created a decision-support model by fusing cognitive mapping with the DEMATEL approach (decision-making trial and evaluation laboratory), as well as by holdinggroup meetings with an expert panel.	The goal of the research was to present a comprehensive knowledge of the potential and difficulties associated with integrating cybersecurity, digital transformation, and AI into the banking industry.	The suggested strategy may be helpful for banking industry decision-makersas they manage the potential and difficulties of integrating new technology while upholding data security and safeguarding their brand.

Senarak, (2020)	A structural approach for preventive andpolicy creationfor port cybersecurity and threat	Utilizing a questionnaire survey and structural equation modeling, three dimensions of port cybersecurity hygiene were developed and their correlations with various cyberthreat categories were examined.	Different sorts of cyberthreats, suchas hacktivism, cybercrime, cyber espionage, cyber terrorism, and cyber war, may be more likely as a result of deficient human, infrastructural, and process elements. Cyberthreats may be avoided with the aid of education and training, better cybersecurity tools, and rigorous adherence to ISPS Code-based protocols.	This study offers port policymakers a framework for creating cybersecurity safeguards and preventing cyberthreats. Port operators should think about making investments in cybersecurity equipment upgrades, training programs, and tight application of preventative measures to safeguard againstvarious cyberthreats.
Rodgers et al., (2019)	The effect of nationality on adherence to cybersecurity controls	Using partial leastsquares structural equation modeling(PLS-SEM) on survey data, it was investigated how foreignness affected internal auditors' adherenceto the International Standards for the Professional Practice of Internal Auditing.	Foreignness has abig influence on how well auditorsfollow the Standards, especially when itcomes to cybersecurity, independence and objectivity, individual objectivity, and governance of the Standards. Foreignness alsohas a big impacton language proficiency and relational socialcapital.	According to thisstudy, external variables like social capital may have an impact on internal auditors' adherence to ethical norms, particularly whenit comes to cybersecurity. The effect of foreignness on compliance should be takeninto account by internal audit departments, andany possible issues should be dealt with.

Hulha et al., (2020)	Banking Information Resource CybersecuritySystem Modeling	Used the techniqueof creating a fuzzycognitive map of the status of bank cybersecurity and created cognitive models to assess the degree of security of the information security system, computer network,and key infrastructure.	The technique makes it possible to forecast the condition of banks' cybersecurity andhelps put requiredsafeguards in place to prevent, protect from, and regulate access atthe proper levels of network infrastructure.	This study offers a technique for evaluating the degree of cybersecurity defense in banks and makes recommendationsfor methods to strengthen control, protection, and preventive measures. This approach should be used by financial organizations so they can recognize their cybersecurity weaknesses and take appropriate action to fix them.
Mishra et al., (2022)	Attributes impacting cybersecuritypolicy development: An evidence from seven nations	Investigated cybersecurity regulations and attributes in the USA, EU, Canada, Australia, China, India, and Malaysia.	Some nations scored higher in managing certaincybersecurity attributes than others. Identifying common policiesacross several nations can assistin developing cybersecurity policies.	This research highlights the importance of having comprehensive cybersecurity policies in placeto address the increasing number of cyberthreats. Governments should consider the common attributes identified in thisstudy when developing their cybersecurity policies and consider how different attributes may beprioritized in different countries.

Fischer-Hübner et al., (2021)	European stakeholder views and cybersecurityneeds	Conducted 63 interviews with European stakeholders working in security-critical industries to identify the most pressing issues, requirements, anddifficulties.	Building trust, implementing privacy and identity management, developing resilient systems, standardization, and certification, attaining security and privacy by design, secure and privacy-compliantdata and information sharing, and government regulations are some of the common issues, challenges, and requirements across sectors.	This study sheds light on the main cybersecurity issues, difficulties, and demands that European stakeholders from diverse security-sensitiveindustries must deal with. This data may be usedby academics andpolicymakers to identify the most important areas for new discoveries and creative solutionsto existing problems.
Fernandez De Arroyabe et al., (2022)	Investing in cybersecurity systems is driven by cyberattacks and cybersecurity skills, according to aUK poll for 2018 and 2019.	To better understand how cyber-capabilitiesand cyber-attacks influence investment in cybersecurity systems, machine learning techniques (ANN and K-mean cluster) were usedto analyze the Cyber Security Breaches Survey data for 4000 firmsfrom 2018 to 2019.	Based on their cybersecurity skills and pastcyberattacks, organizations invest in cybersecurity.	According to thisstudy, while considering whether to invest in cybersecurity systems, businesses should consider both their current cybersecurity capabilities and their prior exposure to cyberattacks. To guide their investment decisions, businesses should constantly evaluate their cybersecurity capabilities and keep tabs on theirexperiences with cyber-attacks.

Gale etal., (2022)	Managing cybersecurityfrom the boardroom: Problems, Motivators, and Future Directions	To better understand existing cybersecurity policies and the elements that influence directors' participation, 18 interviews with non-executive directors from 40+firms were conducted. analyzed data using the neo-institutional theoryas a lens.	Directors' involvement in cybersecurity is primarily influenced by regulations, however they arenot always awareof their responsibilities and liabilities in this area. A director's involvement in cybersecurity is influenced by their individual experiences and backgrounds, and there is sometimes an undue dependence on a single board member who has knowledge in thefield.	This study emphasizes the need for more precise rules andgreater director training on their obligations and liabilities relatedto cybersecurity monitoring. Additionally, it makes a case for the necessity of transparent reporting procedures and diversified cyber experience on theboard. When controlling cybersecurity, organizations should take theseaspects into account.
Gao etal., (2020)	Disclosures of cybersecurity risks by public corporations	Conducted a long-term analysis of the language and content features of cybersecurity risk disclosures made by public firms, aswell as potential driving forces behind disclosure patterns.	The risks of a service/operation being disrupted, and the dangers ofa data breach are the two cybersecurity hazards that are most frequently mentioned. The SEC regulation, industry, general cybersecurity hazards in the environment, firmsize, and historical cybersecurity breach incidencesare all related to the duration of cybersecurity risk disclosures, which grows linearly over time.	The cybersecurity risk disclosure patterns and practices examined in this study are discussed, along with the risks that are revealed and the variables that may affect the scope and style of such disclosures. These results should be taken into account by businesses when they choose the scope and details of their own cybersecurity risk disclosures.

Hillai et al., (022)	Initiatives at the national level to increase cybersecurity education, awareness, and training: Results, Challenges, and Potential	Based on comparative data from 80 countries,a cross-national examination of theeffects of cybersecurity education, awareness raising,and training (CEAT) on internet use was conducted, with contextual factors like affluence and the amount of internet use being taken into account.To determine the main causes of these countries' levels of maturity in this domain, a qualitative study of answers from low-income and developing countries was conducted.	CEAT influencesthe vitality of internet use and services that is both favorable and statistically significant. Regarding CEAT maturity, there are important difficulties for low-income and developing countries. To evaluate the validity of the findings and recommendations for policy and practice, more thorough indicators of CEAT programs across more countries and throughout time are required.	This study emphasizes the value of funding national programs for cybersecurity education, awareness- building, and training in order to enhance internet use and services. When putting these ideas into practice, policymakers and practitioners should take into account the requirements and problems of low-income and developing countries. To completely comprehend the effect of CEAT on internet use and services, more study is required.
Calderon and Gao, (2022)	Corporate cybersecurity risk disclosures have changed as a result of SEC comment letters.	Analyzed the language used in public firms' cybersecurity risk disclosure policiesand the SEC's comment letter policies pertainingto	Only 10% of registrants replyto a comment letter within the advised 10-day window, taking an average of roughly 26 days. 75% of comment letters are handled	According to this research, the SECis crucial to ensure that corporate cybersecurity riskdisclosures are adequate, and corporations may enhance their

		such disclosures. examined how SEC comment letters affect how corporations disclose their cybersecurity risk.	within one communication cycle. Following the discovery of asecurity breach, the SEC carefullyreviews cybersecurity risk disclosures to ensure they are adequate, and it isprobable that it will reject any argument that the incident was not serious. One year after receiving a comment letter, companies alter their disclosure practices, lengthening cybersecurity risk disclosures, making them more precise, andmaking them easier to read andunderstand.	disclosures in response to comment letters. Companies should be aware of the SEC's requirements for disclosures of cybersecurity risks and take action to correct any shortcomings identified in the comment letter.
Hillai et al., (2022)	Initiatives at the national level to increase cybersecurity education, awareness, and training: Results, Challenges, and Potential	Based on comparative data from 80 countries,a cross-national examination of theeffects of cybersecurity education, awareness raising,and training (CEAT) on internet use was conducted, with contextual factors like affluence and the38mountt of internet use being taken into account. To determine the main causes of these countries’	The national viability of internet use and services is positively and quantitatively impacted by CEAT. EffectiveCEAT efforts aredifficult to execute in low- income and developing countries.	To strengthen cybersecurity capabilities and sustain the vitality of internet use and services, policymakers and practitioners should give priority to the nationwide implementation of CEAT programs. When establishing CEAT programs,low-income and developingcountries should take into account their particular difficulties and requirements. To determine more precise markers of CEAT programs and to determine the veracity of these findings, more study is required

		levels of maturity in this domain, a qualitative study of answers from low-income and developing countries was conducted.		
Alawid et al., (2022)	An examination of cybersecurity vulnerabilitiesin the aftermath of COVID-19 in further detail	Data from a globalsurvey of businesses and company leaders between March 2020 and December 2021 were analyzed using a qualitative approach and a multi-criteria decision-making problem-solving strategy.	During the Covid-19 epidemic, cyberattacks weremore frequent and sophisticated, with hacker assaults accounting for 37% of all incidents. Emails, harmful domains, and spam emails were some more common sorts. In order to safeguardagainst future calamities, governments and businesses must be resilient and creative in their cybersecurity decisions.	This study emphasizes the importance of heightened awareness and preventative steps to safeguardagainst cyberattacks in emergency situations. Additionally, it offers particularsuggestions for dealing with typical assault types and highlights the need of continuous efforts to avert crises in the future.
Patel et al., (2022)	A bibliometric assessment of blockchain technology in banking and finance	150+ articles published between2009 and 2021 made up the final sample of a bibliometric evaluation and content analysis of academic literatureon the use of blockchain	The influence of blockchain on financial intermediation, financial applications, regulation and cybersecurity, and sustainable blockchain are some of the major	This study outlines the present status of academic research on blockchain in banking and finance and suggests important topics for further study.

		technology in banking and finance. Co-authorship, cartography, co- citation, and coupling studies were performed on the literature's influential elements, including trending subjects, authors, and target journals.	literature streams highlighted in this study. Examining blockchain regulation, doing cross-country assessments, and using a multidisciplinary approach are the key objectives of future study.	In their own work, practitioners and academics interested in this issue should take into account these streams andthe research agenda.
Prakashet al., (2022)	Text mining literature research of blockchain technology 's use in cybersecur ity	Used automated text mining techniques like subject modelingand keyphrase extraction to analyze the literature of research publications on blockchain technology and cybersecurity.	With blockchain technology comesa number of vulnerabilities, and these risks and weaknesses change as the technology advances. Future directions for developing safe blockchain platforms and applications are provided by this multidisciplinary study.	This study identifies blockchain technology's weaknesses and makes security- improving recommendations . Companies thinking about using blockchain technology should be aware of these weaknesses and take action to fixthem.

Ashiku et al., (2020)	System of Systems (SoS) Architecture for Cybersecurity in Digital Manufacturing	A model was created utilizing the SoS Explorer tool and a genetic algorithm with a fuzzy assessor as a fitness function to choose combinations of protective systemsfor a hypothetical banking cybersecurity issue.	In order to solve cybersecurity issues in digital manufacturing systems, the model produces ameta-architecture.	According to thisstudy, to solve cybersecurity issues in digital manufacturing, aSystem of Systems approach and a variety of protection mechanisms should be used. This technique should be used by manufacturingbusinesses if they want to better safeguard theirsystems from online attacks.
Aseer et al., (2021)	A contingent resource-based examination of real-time analytics, incident response process agility, and corporate cybersecurity performance	specialists were interviewed in-depth, and the dataanalysis employeda contingent resource-based view.	Real-time analytics may help organizationsbe more agile in their incident response procedures, enabling them to respond to sophisticated cyberthreats more quickly and effectively. This might enhance the performance of corporate cybersecurity generally.	Organizations should think about adding real-time analytics capabilities and use them to fosteragility in the incident response process in order to improve incident responseand cybersecurity performance.

Alansari et al., (2021)	E-banking andIT governanc ein GCC-listed banks	Collected information from50+ GCC-registered banks and tested the research model using indices of ITgovernance and e-banking.	The degree of IT governance utilized by GCCregistered banksis strongly correlated with the extent of e-banking in such institutions.	According to thisreport, authoritiesshould help banks by effectively enforcing cybersecurity regulations in theGCC and encouraging the banking industry to use more e- banking tools andapps. Financial institutions in theGCC should think about how IT governance affects their online banking offerings and take action to strengthen IT governanceprocedures.
Sulich et al., 2021)	Sustainabl e Developm entand Cybersecu rity	organizational network theory and study on the connections between cybersecurity andsustainable development examined how cybersecurity is currently being implemented in connection to the Environmental Goods and Services Sector (EGSS) in severalEU nations.	In interorganizational networks, notably in the EGSS, cybersecurity and sustainable development are related and significant challenges. An developing problem in this industry is green cybersecurity, which protects procedures connected to environmental management and protection.	Businesses should think about how cybersecurity fits into sustainable growth, and they should think about putting green cybersecurity safeguards in place to safeguard procedures for environmental management and protection. To assist sustainable production and home security, the EU should give priority to the development of environmental technologies andtheir cybersecurity.

2.10.1 E-Banking And Financial Inclusion

E-banking and financial inclusion may be linked in the sense that e-banking can be used to increase financial inclusion. The ability of individuals and businesses to access and use financial services and products such as banking, credit, and insurance is referred to as financial inclusion. Through electronic and digital technology, e-banking

can provide a convenient and efficient way for individuals and businesses to access financial services, especially in areas where traditional brick-and-mortar branches are not readily available.

Abdi et al. (2022) investigated the impact of automated teller machines (ATMs) and mobile banking on financial inclusion among Somali commercial banks. The researchers used a descriptive survey design to collect primary data from six commercial banks in Somalia that had implemented electronic banking. The study, which used descriptive and inferential statistics, discovered that ATMs and mobile banking were significant predictors of financial inclusion among Somali commercial banks. The study also discovered that electronic banking is important in enabling financial inclusion in commercial banks. This study contributes to a better understanding of financial intermediation theory and the diffusion of innovation theory, as well as the implications for commercial banks and policymakers in promoting financial innovation and increasing financial inclusion.

Dhar (2015) investigated the role of electronic banking in financial inclusion, particularly in the context of India, in their 2015 study. The study used a literature review and secondary data analysis to investigate the scope and challenges of electronic banking and how it can help with financial inclusion in India. According to the findings of the study, electronic banking, including online and mobile banking, can increase financial inclusion by providing access to financial services to people who may not have access to traditional brick-and-mortar bank branches. The study also identified strategies for making electronic banking more personalized and user-friendly in order to maximize benefit for all stakeholders, including financially disadvantaged individuals. This study contributes to a better understanding of the

potential of electronic banking to increase financial inclusion, as well as the challenges that must be overcome to realize that potential.

Ene et al. (2019) conducted another study to investigate the impact of electronic banking on financial inclusion in Nigeria. The total number of ATMs and point-of-sale (POS) devices in the country were used as proxies for electronic banking, and the proportion of the banked adult population to the total bankable adult population was used as a proxy for financial inclusion. According to the study, POS devices have a significant impact on financial inclusion in Nigeria, whereas ATMs do not. Based on their findings, the researchers advised banks to remove barriers to ATM use and strive for international best practices while increasing the availability and accessibility of POS devices for customers. This study contributes to our understanding of the role of electronic banking in increasing financial inclusion, particularly in Nigeria.

Nwude et al. (2020) investigated the role of electronic banking as a tool for financial inclusion in Nigeria in their study. The researchers gathered information from various sources, including the Central Bank of Nigeria's Statistical Bulletin and World Bank economic indicators, to assess the contribution of electronic banking to financial inclusion in Nigeria from 2007 to 2017. The study's findings revealed that electronic banking positively and significantly contributed to the country's financial inclusion. Lack of awareness, distance, poverty, and financial literacy among the rural population were also identified as barriers to implementing electronic banking in Nigeria by the researchers. This study adds to our understanding of electronic banking's potential to increase financial inclusion in developing countries, particularly Nigeria.

2.10.2 E-Banking And Economic Development

E-banking can help economic development by increasing financial inclusion, especially in developing countries where traditional brick-and-mortar bank branches are scarce. E-banking can help to drive economic growth and development by providing access to financial services to individuals who may not have access to traditional banks.

Govender and Wu (2013) surveyed 400 South African consumers to investigate the factors influencing the country's adoption of e-banking. According to the survey findings, perceived usefulness, or the relative advantage of e-banking over traditional banking methods, was a significant factor in adoption. Furthermore, e-banking users perceived it to be less complex and costly than non-users however, social influences had no impact on the adoption of e-banking in South Africa. These findings suggest that efforts to increase e-banking adoption in developing countries should emphasize the perceived benefits and convenience of the service. This can eventually lead to economic development by increasing access to financial services and increasing the potential for e-commerce growth. Gebre (2021) examines the impact of e-banking on commercial bank profitability in Ethiopia between 2011 and 2015. The study used regression analysis to investigate the impact of e-banking services on profitability as measured by return on assets (ROA) and return on equity (ROE) (ROE). ATMs, debit cards, and point of sale were the independent variables studied (POS). The findings indicated that e-banking services had a positive effect on the profitability of Ethiopian commercial banks in terms of both ROA and ROE.

Adoption of e-banking technologies has the potential to contribute to economic development by improving banks' financial performance. The study emphasizes the

importance of considering both technological and organizational factors when implementing e-banking services,as well as the regulatory environment's role.

2.10.3 E-Banking And Customer Behavior

In the context of e-banking, consumer behavior refers to the actions and decisions that individuals make regarding their use of e-banking services. Wachyudhi and Budi Haryanto (2016) conducted a study to investigate the behavior of consumers who intended to continue using e-banking services. Variables such as perceived relationship marketing, electronic service quality (e-serqual), consumer satisfaction, trust, and perceived switching costs were included in the study's model. The study's data came from 200 e-banking users, specifically business administration students at Indonesia's Krisnadwipayana University.

The findings of the study revealed a reciprocal and mutually beneficial relationship between perceived relationship marketing and e-sequel. Furthermore, e-sequel increased both consumer satisfaction and trust. However, neither perceived relationship marketing nor e-sequel had a direct or indirect effect on consumer continued intention to use e-banking via satisfaction and trust. Instead, perceived switching costs had a significant moderating effect on consumer intentions to continue using e-banking.

According to the study's findings, while factors like relationship marketing and e-sequel are important for e-banking service providers to consider, themagnitude of perceived switching costs may be a more influential factor in determining consumer behavior with e-banking. This study sheds light on the complex factors that can influence consumer behavior in the context of e-banking, with implications for both theory and practice in this field.

According to the study’s findings, e-banking security and privacy, responsiveness, and reliability all had a significant impact on customer satisfaction. In contrast, usability had no significant impact. These findings are useful for e-banking service providers looking to improve their offerings and ensure customer satisfaction. This study adds to the existing body of knowledge about customer satisfaction in e-banking, specifically in Malaysia. Kerem (2003) investigated the factors influencing the adoption of e-banking as a primary banking channel in Estonia, a country known for its openness to new technologies. The study specifically sought to understand the impact of demographic factors and attitudes toward banking-related issues on choosing a primary banking channel, the characteristics of heavy e-banking users and the barriers to further adoption, and the critical success factors of Estonian e-banking. Based on the innovation diffusion theory, the study used a survey of bank customers as well as interviews with leading banking professionals and industry experts.

According to the study's findings, the success of e-banking, particularly Internet banking, is influenced by a complex combination of factors such as bank activities, general infrastructure, the economic environment, and government initiatives. The study also discovered that, while e-banking adoption rates in Estonia are high compared to other East European countries and comparable to adoption rates in Scandinavian countries, there is still room for growth. One limiting factor is limited internet access among certain customer groups, resulting in a digital divide. The study also discovered that, while banks' marketing activities were not viewed as critical in the adoption decision, more than just advertising may be required to persuade non-users of Internet banks to begin using the services. These findings provide insight into the factors that influence e-banking adoption and the challenges that may need to be addressed to increase adoption rates.

2.10.4 E-Banking And Financial Literacy

In recent years, e-banking, also known as internet banking or online banking, has grown in popularity as a financial service. Individuals can use a digital platform to access and manage their financial accounts, including making payments and transferring money. As e-banking becomes more common, it is critical to consider the role of financial literacy in the use of these services by individuals.

According to Andreou and Anyfantaki (2020), financial literacy has a significant impact on individuals' use of e-banking in Cyprus. The study discovered a link between financial knowledge and the frequency with which people use e-banking. Financially illiterate consumers, on the other hand, were more likely to cite a lack of trust in e-banking as well as a lack of confidence in their financial and digital skills as reasons for not usingthe service. These findings emphasize the importance of financial literacy in enabling individuals to effectively use and benefit from e-banking services. Furthermore, the study emphasizes the importance of individuals having financial literacy and digital proficiency in order to fully participate in the digital economy. Ionescu (2021)conducted desk research to analyze data on financial literacy, digital literacy, financialbehavior, and digital technology adoption in the EU. The study discovered that there may be differences in financial literacy and digital literacy levels across EU member countries.

Furthermore, the study discovered that, while EU citizens have a generally positive attitude toward FinTech solutions and digital money, there is still a need for more knowledge and understanding of cryptocurrencies. These findings highlight the importance of ongoing financial education and information in the digital age, particularly in the rapidly evolving financial technology industry. Hogarth and

Anguelov (2004) investigated a demonstration program aimed at increasing financial literacy and access to information and communication technologies among low- and moderate-income people in inner-city areas. While the program had no overall significant effects, there was evidence of a potential link between access to information and communication technologies and financial literacy, according to the study.

According to the authors, implementation issues have harmed the program's effectiveness. However, the study discovered that urban low- and moderate-income people wanted to become more technologically and financially literate, and that an intensive intervention may be required to achieve these goals. These findings emphasize the critical importance of addressing the digital divide and financial literacy issues in order for disadvantaged groups to fully participate in the financial mainstream and benefit from electronic banking technologies. To improve adoption among younger adults, Koya et al. (2021) conducted a survey and interviews to investigate the usability of UK digital banking services. According to the study, younger adults found the current user interfaces of digital banking applications difficult to navigate and required more personalized information.

Furthermore, their lack of financial knowledge and information discouraged them from utilizing various features and products made available digitally by banks. According to the authors, incorporating accessible financial information and personalized elements into the design of digital banking applications, as well as offering incentives, could increase adoption rates among younger adults. This study emphasizes the significance of financial literacy in the design and promotion of digital banking services, particularly for younger adults who may need to become more acquainted with financial concepts and terminology. Dilek and colleagues (2015).

2.10.5 The Role Of Technology In Preventing And Detecting Cybercrime In E-Banking

Technology is critical in the prevention and detection of cybercrime in e-banking. Technology aids in the prevention of cybercrime by utilizing secure servers and encryption techniques that prevent unauthorized parties from accessing sensitive financial information. Furthermore, advanced authentication methods such as two-factor authentication and biometric verification can improve security and lower the risk of cyber-attacks.

On the detection front, artificial intelligence and machine learning algorithms can assist in identifying and tracking suspicious activity. These algorithms are capable of analyzing large amounts of data and identifying patterns or anomalies that may indicate a cyber-attack. In this way, technology assists financial institutions in remaining vigilant and responding quickly to any potential threats.

2.10.6 Artificial Intelligence and Machine Learning

In the fight against cybercrime, artificial intelligence (AI) is becoming increasingly important. Traditional monitoring and protection methods have yet to be completely successful in protecting cyber infrastructures. Artificial neural networks and fuzzy logic, for example, are effective at detecting and preventing cyber-attacks. These techniques are used in a variety of applications, such as intrusion detection systems, spam detection, and malware classification. Furthermore, AI can be used to create software and machines that think and behave like humans, allowing for more efficient decision-making in the face of cyber-attacks (Dilek et al., 2015). Intelligent agents, computer programs that can analyze and respond to attacks in real time, are one promising application of AI in combating cybercrime. These agents can be programmed to detect and analyze potential attacks, as well as to take appropriate

defensive action. They can also be used to devise prevention strategies for secondary attacks.

Another area where AI has shown promise is in the use of artificial immune systems (AIS). These systems, which mimic a living organism's immune system, can be used to detect and respond to threats in a cyber environment. AISs have been used in anti-virus technology and have demonstrated promise in detecting and preventing a variety of cyber-attacks, such as denial of service (DoS) attacks and computer worms.

There are also several challenges to using AI to combat cybercrime. One major issue is the ongoing need for AI system updates as cybercriminals develop new attack methods. Furthermore, there are concerns about the potential for AI systems to be used for malicious purposes, as well as the need for effective risk management to prevent this.

Overall, the use of AI in combating cybercrime is a rapidly expanding field with significant potential for improving cyberinfrastructure security. More research and development in this area is required to fully realize the benefits of AI in combating these threats.

According to Madan L. Bhasin (2016), the regulations and laws governing India's financial services sector are constantly changing. Bhasin (2016) identifies the Reserve Bank of India Act of 1934, the Securities and Exchange Board of India Act of 1992, the Companies Act of 2013, the Prevention of Money Laundering Act of 2002, and the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act of 2015.

2.10.7 Biometric Authentication

Biometrics, according to Pricop (2021), can improve the security of industrial control systems (ICSs) in the face of significant cyber threats. An ICS decoy attracted 1,300 attempts to gain unauthorized access within a month, according to a Kaspersky Lab study. Biometric technology, when implemented, can provide security for critical industrial facilities such as petrochemical plants, refineries, and power plants.

Santoso (2019) found that biometric technology, such as fingerprint technology, can play an important role in protecting consumer identity during online banking transactions. As the number of online banking scams grows, implementing biometric technology can provide objective evidence for law enforcement in cyberspace and aid in the detection of authorized users.

Santoso (2019) discovered three methods for protecting consumer identity through biometric validation in banking security regulation, government regulation on consumer identity protection, and consumer behavior in maintaining their identity. These findings highlight the significance of incorporating biometric technology into online banking to improve security and protect customers from identity theft. Biometric technology, such as fingerprinttechnology, can protect consumer identity during online banking transactions, according to Santoso (2019). As the number of online banking scams grows, implementing biometric technology can provide objective evidence for law enforcement in cyberspace and aid in the detection of authorized users. Santoso (2019) discovered three methods for protecting consumer identity through biometric validation in banking security regulation, government regulation on consumer identity protection, and consumer behavior in maintaining their identity. These findings highlight the significance of incorporating biometric

technology into online banking to improve security and protect customers from identity theft.

2.10.8 The Role Of Government And Regulatory Bodies In Addressing Cybercrime In E-Banking

The Financial Stability Institute's article, "Regulatory approaches to enhance banks' cyber-security frameworks" (Crisanto & Prenio, 2017), discusses the various approaches taken by governments and regulatory bodies in Hong Kong, Singapore, the United Kingdom, and the United States to combat cyber-crime in e-banking. The authors investigate the existing essential regulatory requirements for cyber risk, as well as the various supervisory frameworks and tools in place in these jurisdictions. The article also makes observations about how the banking industry is implementing these regulations and offers policy considerations for addressing cybercrime in e-banking.

This article provides useful insight into the role of government and regulatory bodies in combating cybercrime in e-banking, as well as the various approaches taken in different countries. In their article "Follow the leaders: How governments can combat intensifying cybersecurity risks," Fadia, Nayfeh, and Noble (2020) examine the challenges of developing and implementing a national cybersecurity strategy in the face of state-sponsored cyber warfare and rising cyber threats.

Five common elements of successful national strategies are identified by the authors: a dedicated national cybersecurity agency, a National Critical Infrastructure Protection program, a national incident response and recovery plan, clearly defined laws governing all cybercrimes, and a thriving cybersecurity ecosystem.

Governments need these strategies to prevent cyberattacks, mitigate damage, and protect their citizens, businesses, and critical infrastructure. The authors also discuss the importance of developing a cybersecurity culture and the need for international cooperation to combat global cyber threats. Thisarticle provides valuable insight into governments' roles in addressing the growing threat of cybercrime and the strategies they can use to combat it. Taylor (2022) discusses the long-standing issue of cybersecurity in the US federal government, as well as the various initiatives and policies that have been implemented to address it.

Despite these efforts, the federal government has experienced numerous cyber disasters, including the Office of Personnel Management data breach in 2015 and the SolarWinds hack in 2020, which exposed every system in the government to unauthorized access. In response to these challenges, the Biden administration has proposed a $2 trillion infrastructure spending bill that includes funding for critical infrastructure upgrades and addressing supply chain vulnerabilities, as well as $9.8 billion for federal agencies to improve their cybersecurity. The article also discusses the role of various federal agencies in cybersecurity, such as the National Security Agency and the Department of Homeland Security, as well as the efforts of standards bodies and private companies to combat cyber threats.

This article provides a thoroughoverview of the challenges and efforts to address cybersecurity in the federal government of the United States.

2.11 Cybersecurity Measures Used By E-Banking Systems

To protect against unauthorized access and cyber-attacks, e-banking systems employ a variety of cybersecurity measures. One standard measure is to use strong passwords

that must be changed on a regular basis and are not easily guessable. Another security measure is to use two-factor authentication, which requires more than just a password. A code sent to a user's phone or a physical token could be used. E-banking systems may also employ encryption to safeguard data transmitted over the internet, as well as firewall technologies to prevent unauthorized access. Furthermore, e-banking systems frequently have systems in place to monitor and detect suspicious activity, such as unusual login attempts or large financial transactions. E-banking systems use these and other cybersecurity measures to protect sensitive financial information while also ensuring the security and trust of their users.

In a recent article titled "China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems," Lundvall and Rikap (2021) investigate China's emergence as a leader in the field of artificial intelligence (AI) and the role of innovation systems in this process. According to the authors, China's success in AI can be attributed to the co-evolution of corporate and national innovation systems, with tech behemoths like Alibaba and Tencent playing a significant role in this process. These companies have drawn on knowledge sources within China's national innovation system while also collaborating with international partners and organizing R&D activities outside of China's borders. According to the authors, this combination of domestic and international collaborations has not only strengthened China's geopolitical position but has also posed a challenge to the Chinese state's control over the economy. Lundvall and Rikap (2021).

2.12 Case Studies Of Cyber-Attacks On E-Banking Systems

In her article "A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches," Xiang Michelle Liu (2021) investigates the

vulnerabilities in the international banking system as well as the channels through which advanced persistent threats (APTs) can be delivered. The author focuses on the SWIFT messaging network, which has had a number of data breaches in recent years.

To protect against APTs, Liu emphasizes the importance of financial institutions implementing effective governance mechanisms and incorporating risk management processes into their cybersecurity strategies. The study also recommends that financial institutions form global alliances to better protect themselves against cyber threats.The SWIFT network has been vulnerable to cyberattacks due to its rapid growth and expansion, which has outpaced the implementation of cybersecurity measures, according to one key finding of the study. Millions of dollars have been lost as a result, as well as the reputation and customer confidence of the affected institutions. To address these vulnerabilities, the author recommends that financial institutions implement a risk management framework, such as the SWIFT Customer Security Control Program, which includes risk assessments, security controls implementation, and continuous threat monitoring.

Liu also examines existing cybersecurity regulations and industry practices in the banking and payments sector, as well as the countermeasures implemented by SWIFT in response to data breaches. The study concludes with a discussion of the lessons learned from these cases and future research directions for improving financial industry cybersecurity. (Liu, 2021).

In a number of high-profile attacks, cybercriminals exploited vulnerabilities in the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network. These attacks frequently involved the use of malware to gain access to bank networks

and employee credentials, which were then used to manipulate transaction data and transfer funds to controlled accounts. In some cases, the attackers used cutting-edge technology to gain access to the banks' networks, while in others, they exploited flaws in the banks' security measures. The 2013 attack on Sonali Bank in Bangladesh, in which keyloggers were used to steal employee credentials and $250,000 was lost; the 2015 attack on Banco del Austro in Ecuador, in which $12 million was lost; and the 2016 attack on the Bangladesh Central Bank, in which $81 million was lost, are among the most notable SWIFT network attacks. These attacks highlight the ongoing threat that cybercriminals pose to payment systems, as well as the need for stronger security protocols across financial institutions. (Liu, 2021).

Malware was found to be a key component in many of the attacks in a case study of cyber-attacks on financial messaging networks. This could be due to anti-malware software that is out of date or software that has been set to periodic detection mode for performance reasons. Pirated software has also been identified as a major vulnerability for financial institutions, as it prevents the installation of new patches or upgrades and impedes the development of robust IT infrastructure. Human error, as well as a lack of proper protocols and risk management processes, contributed to successful attacks in addition to technological vulnerabilities. Poor firewall protection and the use of a second-hand network switch worth $10 were identified as weaknesses in the Bangladesh Bank heist, and pirated software was purchased from untrustworthy vendors in the NIC Asia Bank case. Recovery of stolen funds is also a difficult process, as in the Bangladesh Bank case, the stolen money vanished after arriving in the Philippines and Sri Lanka and was spread into casinos, making recovery difficult due to the Philippines' limited anti-money laundering laws. Individual banks, as well as the financial messaging network, SWIFT, share responsibility for preventing and

defending against cyber-attacks.

2.13 Best Practices For E-Banking Security

The authors of Wodo et al article's "Evaluating the Security of Electronic and Mobile Banking" discuss the importance of evaluating the security of e-banking systems in order to protect against cyber threats. They identify several assessment areas to consider, such as login and transaction confirmation/authorization, data protection and analysis, and form design, and use these areas to create a survey to evaluate the security of Polish banks. The authors discovered that while all of the banks studied had a transaction limit set by default, the maximum limits varied significantly. They also discovered that only a few banks used two-factor authentication by default for mobile applications, and that none of the banks provided users with security reports.

Furthermore, the authors discovered that banks did not assess a user's account security beyond the strength of their password. The authors conclude that improved security measures in e-banking systems, such as the use of two-factor authentication and the distribution of security reports to users, are required. They also advocate for the development of guidelines for evaluating the security of e-banking systems in order to ensure that these services are used safely and responsibly.

Using strong passwords and regularly updating them is one of the best practices for e-banking security. This can aid in the prevention of unauthorized account access and the confidentiality of personal and financial information. It is also critical to use different passwords for different accounts and to avoid using passwords that are easily guessable, such as personal information or common words. Another recommended practice is to use two-factor authentication when logging in and completing

transactions (2FA).

Adding an extra layer of protection by requiring the use of a second form of authentication, such as a code delivered to a cell phone or a fingerprint scan. When accessing e-banking services, it is also recommended to use secure networks, such as a virtual private network (VPN) or a secure Wi-Fi connection. This can help prevent hackers and other third parties from intercepting data. Furthermore, it is criticalto keep software and security measures on e-banking devices up to date. This can assist in protecting against vulnerabilities and ensuring that the most recent security features are used.

Finally, when using e-banking services, it is best to be cautious and avoid clicking on suspicious links or providing personal or financial information to unknown parties. It is also critical to be aware of common scams, such as phishing attacks, and to immediately report any suspicious activity to the bank (citations). These are some of the best practices available in the literature for helping individuals protect themselves and their accounts from cyber threats.

2.14 The Role Of Customer Education In Preventing Cybercrime In E- Banking

Customer education, according to Sanders and Berenbeim (2018), is critical in preventing cybercrime in e-banking. The study focuses on Frontline Service Employees (FSEs) in the banking industry, who play an important role in providing customers with cyber security information. According to the study, FSEs generally have little knowledge about the consequences of cybercrime, but their experiences can help them provide basic information to customers. FSEs use their experiences and

problem-focused coping strategies to combat the threat of cybercrime, such as attempting to learn more about the situation and focusing on the next step in providing the best possible service to the customer.

According to the study, banks should consider offering special courses to educate FSEs about the consequences of cybercrime so that they can provide customers with more specific information about how to protect themselves. According to Khatri (2019), the banking sector has been atarget for cyber-attacks for several years. The increased reliance on digital networks and online transactions has increased the risk of data breaches and cybercrime.

Cybersecurity in the banking sector is critical for protecting customer assets and preventing trust in financial institutions from eroding. Some of the current risks associated with online banking include an increased risk of mobile app attacks, breaches at third-party organizations, and an increased risk of cryptocurrency hacks. Banks should consider implementing a thorough security audit, updated firewalls, anti-virus and anti-malware applications, and multi-factor authentication measures to protect themselves against these attacks.

Furthermore, banks can improve their cybersecurity by educating their employees about the importance of cybersecurity, providing customers with clear and concise information about protecting their assets, and reviewing and updating their cybersecurity policies and procedures on a regular basis.

2.15 The Psychological Impact Of Cybercrime On E-Banking Customers

People are more likely to respond to the effects of a cyber-attack than the attack itself, according to Bada and Nurse (2020) in their article on the social and psychological impact of cyber-attacks. For example, in the event of a cyber-attack in which malware infects a national power station, the public may be more concerned about the consequences of being without power, such as being unable to heat their homes or prepare food.

Bada and Nurse investigate the social and psychological (emotional andbehavioral) consequences of cyber-attacks, such as the social disruption caused to daily lives and the widespread issues of anxiety or loss of confidence in technology, as well as more personal psychological consequences such as anxiety, worry, anger, and depression. They also discuss the role of risk perception and protection motivationin shaping an individual's response to a cyber-attack, as well as the impact of culture and attacker characteristics on public response. Bada and Nurse provide insight into the social and psychological impacts of cyber-attacks by examining two significant cyber-attacks, the WannaCry attack in 2017 and the Lloyds Banking Group attack, andthe importance of understanding these impacts in order to effectively address and mitigate their effects.

The study concluded that understanding the social and psychological effects of cyber-attacks on members of the public is critical in order to improve our understanding of the broader side effects of attacks. The study also suggested that more research into the interaction of cybersecurity and cognitive factors is required.

Chapter 3

CONCLUSION

To summarize, cybercrime has a significant and multifaceted impact on e-banking. Cybercrime can put e-banking systems and the financial information of individuals and businesses that use these services at risk. E-banking and financial inclusion are intertwined in the sense that e-banking can provide access to financial services in areas where traditional brick-and-mortar branches may not exist. Individuals' use of e-banking is influenced by their financial literacy, with those who are financially literate more likely to use and benefit from the service. The US federal government has faced significant cybersecurity challenges and has implemented a variety of initiatives and policies to address these issues. However, cyber disasters such as the Office of Personnel Management data breach in 2015 and the SolarWinds hack in 2020 highlight the ongoing need for effective cybersecurity measures. To ensure the safety and security of e-banking systems and users' financial information, e-banking providers and governments must prioritize cybersecurity.

Furthermore, the role of financial intermediaries in e-banking, as well as the adoption of financial innovation, plays a significant role in the effects of cybercrime on e-banking. As e-banking becomes morecommon, financial intermediaries must consider the risks and potential vulnerabilitiesof e-banking systems and implement mitigation measures. Policymakers must also encourage the use of financial innovation and increase financial inclusion through e- banking. To effectively address the effects of

cybercrime on e-banking, all stakeholders must collaborate and prioritize cybersecurity measures. Overall, the research presented in this paper emphasizes the importance of understanding the effects of cybercrime on e-banking, as well as the need for effective risk-mitigation measures. E-banking can provide quick and easy access to financial services, especially in areas where traditional branches are not available. However, e-banking providers and governments must prioritize cybersecurity to ensure the safety and security of these systems and users' financial information. In addressing the effects ofcybercrime on e-banking, financial literacy and the role of financial intermediaries arealso important factors to consider.

This research has added to the literature by shedding light on the consequences of cybercrime on e-banking and the importance of adequate risk-mitigation techniques. Furthermore, the article focused attention on the importance of financial literacy and the role of financial intermediaries in mitigating the impacts of cybercrime. Although e-banking can enable speedy access to banking services, it is crucial to take precautions to ensure the confidentiality of consumers' personal accounts.

To mitigate the consequences of cybercrime on e-banking, stakeholders must continue to work and prioritize cybersecurity measures in the future. Furthermore, institutions play a critical role in increasing financial literacy among users. They should continuously aim to educate the consumer on the necessity of cyber security measures, which may assist them in better protecting their data and assets. Finally, governments may assist to build a safe and secure e-banking environment for everybody by providing financial intermediaries with the expertise and resources needed to identify and manage possible risks.

REFERENCES

Abdi, A., Hussein, F., & Kadir, H. (2022). Effect of electronic banking on financial inclusion among commercial banks in Somalia. *International Journal of Financeand Accounting, 7*(2), 43–54. https://doi.org/10.47604/ijfa.1547

Aduba, J. J. (2021). On the determinants, gains and challenges of electronic banking adoption in Nigeria. *International Journal of Social Economics*, 48(7), 1021–1043. https://doi.org/10.1108/ijse-07-2020-0452

Alansari, Y., & Musleh Al-Sartawi, A. M. A. (2021). It governance and e-banking in GCC listed banks. *Procedia Computer Science, 183,* 844–848. https://doi.org/10.1016/j.procs.2021.03.008

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Anan, L., Chen, J., Mahajan, D., & Nadeau, M. C. (2022). Consumer trends in digital payments. *McKinsey & Company*. Retrieved December 30, 2022, from https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-trends-in-digital payments

Andreou, P. C., & Anyfantaki, S. (2019). Financial literacy and its influence on consumers' internet banking behaviour. *SSRN Electronic Journal*.

https://doi.org/10.2139/ssrn.3499104

Ashiku, L., & Dagli, C. H. (2019). System of systems (SOS) architecture for digital manufacturing cybersecurity. *Procedia Manufacturing*, *39*, 132–140. https://doi.org/10.1016/j.promfg.2020.01.248

Ashraf, M., Jiang, J. (X., & Wang, I. Y. (2022). Are there trade-offs with mandating timely disclosure of cybersecurity incidents? evidence from state-level data breach disclosure laws. *The Journal of Finance and Data Science*, *8*, 202–213. https://doi.org/10.1016/j.jfds.2022.08.001

Bada, M., & Nurse, J. R. C. (2019/20). The social and psychological impact of cyber-attacks. *In Benson & McAlaney* (Eds.), Emerging cyber threats and cognitive vulnerabilities (pp.). Academic Press.

Bennett, R., & Bennett, K. (2022). Digital Banking in 2022: trends and statistics. bank rate. Retrieved December 30, 2022, from https://www.bankrate.com/banking/digital-banking-trends-and-statistics/#digital-trends

Bhasin, Madan L. (2016). The role of technology in combatting bank frauds: perspectives and prospects. eco forum, 5(2), 200-212.

Calderon, T. G., & Gao, L. (2022). Changes in corporate cybersecurity risk disclosures after SEC comment letters. *Journal of Accounting and Public Policy*,*41*(5), 106993. https://doi.org/10.1016/j.jaccpubpol.2022.106993

Calderon, T. G., & Gao, L. (2022). Changes in corporate cybersecurity risk disclosures after SEC comment letters. *Journal of Accounting and Public Policy*,*41*(5), 106993. https://doi.org/10.1016/j.jaccpubpol.2022.106993

Coman, D. M., Ionescu, C. A., Duică, A., Coman, M. D., Uzlau, M. C., Stanescu, S. G., & State, V. (2022). Digitization of accounting: the premise of the paradigm shift of role of the professional accountant. *Applied Sciences*, 12(7), 3359. https://doi.org/10.3390/app12073359

Crisanto, J. C., & Prenio, J. (2017). Regulatory approaches to enhance banks' cyber-security frameworks. *Bank for International Settlement*, *1*(02).

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*, 37(1), 1–29. https://doi.org/10.1007/s10869-021-09732-9

Dhar, S. K. (2015). Role of electronic banking in financial inclusion. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2574608

Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: a review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102

E-banking.(n.d.).Toprr.https://www.toppr.com/guides/business-economics-cs/money-and-banking/e-banking/

Ene, E. E., Abba, G. O., & Fatokun, G. F. (2019). The impact of electronic banking on financial inclusion in Nigeria. *American Journal of Industrial and Business Management*, *09*(06), 1409–1422. https://doi.org/10.4236/ajibm.2019.96092

Fadia, A., Nayfeh, M., & Noble, J. (2022, September 1). Follow the leaders: How governments can combat intensifying cybersecurity risks. *McKinsey & Company*. Retrieved December 30, 2022, from https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*, *124*, 102954. https://doi.org/10.1016/j.cose.2022.102954

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*, 102916. https://doi.org/10.1016/j.jisa.2021.102916

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the board room: challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management &Amp; Computer Security*, 11(2), 74–83. https://doi.org/10.1108/09685220310468646

Gebre, B, (2017). The effects of e-banking on bank performance. The case of selected Ethiopian commercial banks, Munich, GRIN Verlag, https://www.grin.com/document/999910

Govender, J. P., & Wu, J. (2013). The adoption of internet banking in a developing economy. *Journal of Economics and Behavioral Studies*, *5*(8), 496–504. https://doi.org/10.22610/jebs.v5i8.423

Grover, P., Kar, A.K. and Janssen, M. (2019), Diffusion of blockchain technology: Insights from academic literature and social media analytics, *Journal of Enterprise Information Management*, Vol. 32 No. 5, pp. 735-757. https://doi.org/10.1108/JEIM-06-2018-0132

Hassink, H., de Vries, M., & Bollen, L. (2007). A content analysis of whistleblowing policies of leading european companies. *Journal of Business Ethics*, 75(1), 25–44. https://doi.org/10.1007/s10551-006-9236-9

Jain, J. (2021). Artificial intelligence in the cyber security environment. *Artificial Intelligence and Data Mining Approaches in Security Frameworks*, 101–117. https://doi.org/10.1002/9781119760429.ch6

Kerem, K. (2003). Adoption of electronic banking: underlying consumer behaviour and critical success factors.

Khatri, P. (2019). The importance of cyber security in banking. The global treasurer. Retrieved from https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/

Koya, K., Matrix Consultant,.V, & Jones, D. (2021). A path of roses and financial literacy: Exploring the usability of UK's digital banking services to improve younger adult adoption. 2021 3rd Asia *Pacific Information Technology Conference*.https://doi.org/10.1145/3449365.3449369

Kroll, J., Mäkiö, J., & Assaad, M. (2016). Challenges and practices for effective knowledge transfer in globally distributed teams - a systematic literature review. Proceedings of the 8th international joint conference on knowledge discovery, knowledge engineering and knowledge management. https://doi.org/10.5220/0006046001560164

Leung, R. (2018, May 1). Cybersecurity regulation in the banking sector: global emerging themes. Research Gate. https://www.researchgate.net/publication/328419728_Cybersecurity_regulation%20%20_in_the_banking_sector_global_emerging_themes

Liébana-Cabanillas, F., Muñoz-Leiva, F., & Rejón-Guardia, F. (2013). The determinants of satisfaction with e-banking. *Industrial Management &Amp; Data Systems*, 113(5), 750–767. https://doi.org/10.1108/02635571311324188

Liébana-Cabanillas, F., Muñoz-Leiva, F., Sánchez-Fernández, J., & Viedma-del Jesús, M. I. (2015). The moderating effect of user experience on satisfaction with electronic banking: empirical evidence from the Spanish case. *Information Systems and E-Business Management*, 14(1), 141–165. https://doi.org/10.1007/s10257-015-0277-4

Liu Xian,. M (2021) A risk-based approach to cybersecurity: a case studyof financial messaging networks data breaches, *The Coastal BusinessJournal:* Vol. 18: No. 1, Article 2. Available at: https://digitalcommons.coastal.edu/cbj/vol18/iss1/2

Lundvall, B.-Å., & Rikap, C. (2022). China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. *Research Policy*, *51*(1), 104395. https://doi.org/10.1016/j.respol.2021.104395

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: empirical evidence. *Research in Economics*, *76*(2), 131–140. https://doi.org/10.1016/j.rie.2022.07.001

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security, 120,* 102820. https://doi.org/10.1016/j.cose.2022.102820

Mulia, K. (2021, October 8). 4 key stats from finder's report on digital banking adoption. *KrASIA.* https://kr-asia.com/4-key-stats-from-finders-report-on-digital-banking-adoption

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Masood Siddiqui, A. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management, 59,* 102334. https://doi.org/10.1016/j.ijinfomgt.2021.102334

Nazaritehrani, A., & Mashali, B. (2020). Development of e-banking channels and market share in developing countries. *Financial Innovation*, *6*(1). https://doi.org/10.1186/s40854-020-0171-z

Ndlovu, I., & Ndlovu, M. (2013). Mobile banking the future to rural financial inclusion: case study of Zimbabwe. *IOSR Journal Of Humanities And Social Science*, 9(4), 70-75.

Nwude, C. E., Igweoji, N. D., & Udeh, S. N. (2020). The role of electronicbanking as a tool to financial inclusion in Nigeria. *Noble International Journal of Business and Management Research*, *04*(01), 01–08. https://doi.org/http://napublisher.org/?ic=journals&id=2

Nur, A. M. (2022). The role of digital banking services on commercial banks performance in Somalia: a descriptive and ols approach. *International Journal of Financial Research*, 13(4), 16. https://doi.org/10.5430/ijfr.v13n4p16

Patel, R., Migliavacca, M., & Oriani, M. E. (2022). Blockchain in banking and finance: A bibliometric review. *Research in International Business and Finance*, *62*, 101718. https://doi.org/10.1016/j.ribaf.2022.101718

Prakash, R., Anoop, V. S., & Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights*, *2*(2), 100112. https://doi.org/10.1016/j.jjimei.2022.100112

Pricop, E. (2019). Biometrics the secret to securing industrial control systems. *Biometric Technology Today*. https://doi.org/10.1016/s0969-4765(19)30054-2

Priyadarshini, I., & Sharma, R. (2022). Artificial Intelligence and Cybersecurity: Advances and Innovations. CRC Press.

Răzvan, I. (2021). Financial literacy in the digital age. *Revista Estrategia Organizacional*, *10*(2). https://doi.org/10.22490/25392786.4958

Rodgers, W., Alhendi, E., & Xie, F. (2019). The impact of foreignness on the compliance with cybersecurity controls. *Journal of World Business*, *54*(6), 101012. https://doi.org/10.1016/j.jwb.2019.101012

Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation, and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, 60, 101616. https://doi.org/10.1016/j.ribaf.2022.101616

Santoso, E, et al. (2019). The role of biometric technology to protect consumer in onlinebanking transaction. *International Journal of Advanced Science and Technology*, 28(20), 526 - 533. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/2843

Sanders, J., & Berenbeim, R. (2018). The role of customer education in preventing cybercrime in e-banking. *Journal of Financial Crime*, 25(3), 1020-1030. doi:10.1108/JFC-09-2017-0072

Senarak, C. (2021). Cybersecurity knowledge and skills for port facility security officers of international seaports: perspectives of it and security personnel. *The Asian Journal of Shipping and Logistics*, *37*(4), 345–360. https://doi.org/10.1016/j.ajsl.2021.10.002

Senarak, C. (2021). Port Cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics*, *37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

Servon, L. J., & Kaestner, R. (2008). Consumer financial literacy and the impact of online banking on the financial behavior of lower-income bank customers. *The Journal of Consumer Affairs*, 42(2), 271–305.

http://www.jstor.org/stable/23859645

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: national level evidence-based results, challenges, and promise. *Computers & Security*, *119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking information resource cybersecurity system modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), 80. https://doi.org/10.3390/joitmc8020080

Sipola, T., Kokkonen, T., & Karjalainen, M. (2023). Artificial intelligence and cybersecurity: theory and applications. *Springer Publishing.*

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards, and recommendations. *Future Generation Computer Systems*, 92, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Stoica, O. C., & Ionescu-Feleagă, L. (2021). Digitalization in accounting: a structured literature review. *Resilience and economic intelligence through digitalization and big data analytics*, 453–464. https://doi.org/10.2478/9788366675704-045

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science*, *192*,

20–28. https://doi.org/10.1016/j.procs.2021.08.003

Taylor, H. (2022, November 10). Cybersecurity in federal government. *Cybersecurity Guide*. Retrieved December 30, 2022, from https://cybersecurityguide.org/industries/government/

Tian, S., Zhao, B., & Olivares, R. O. (2022). Cybersecurity risks and central banks' sentiment on central bank digital currency: evidence from global cyberattacks. *Finance Research Letters*, 10360 https://doi.org/10.1016/j.frl.2022.103609

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/j.irfa.2021.101795

Wachyudhi, N., & Haryanto, B. (2016). E-banking and consumer behavior: The role of switching costs. *Corporate Ownership and Control*, *13*(3), 234–249. https://doi.org/10.22495/cocv13i3c1p10

Wodo, W., Blaskiewicz, P., Stygar, D., & Kuzma, N. (2021). Evaluating the security of electronic and mobile banking. *Computer Fraud & Security*, *2021*(10), 8–14.https://doi.org/10.1016/s1361-3723(21)00107-x

Yusuf Dauda, S., & Lee, J. (2015). Technology adoption: A conjoint analysis of consumers ′preference on future online banking services. *Information Systems*, 53, 1–15. https://doi.org/10.1016/j.is.2015.04.006