Annu-Maria Keränen

RISING CYBER THREATS TARGETING THE BANKING SECTOR

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2022

ABSTRACT

Keränen, Annu-Maria
Rising cyber threats targeting the banking sector
Jyväskylä: University of Jyväskylä, 2022, 34 pp.
Information Systems science, bachelor's thesis
Supervisor: Mehtälä, Saana

The development of technology leads to new innovations in both business and everyday life. As technology progresses, so do cyber threats. The stability and security of the banking sector need to be ensured because it is a part of society's critical infrastructure. The cyber threats targeting the banking sector must be studied to maintain the confidence in the financial system. The goal of this literature review was to define the relevant cyber threats that banks are facing and how they might evolve in the future. Banking operations that are especially prone to cyber threats and the technologies that are utilized in banking operations were examined. Cyber threats and their future development were considered. In addition, the expanding financial technology industry and the potential threats arising from it were reviewed. This thesis was based on previous literature on the banking industry, cybersecurity in banks, and financial technology. It was found that the most relevant cyber threats that the banks are facing are cybercrime threats and insider threats. In addition to these, vulnerabilities in information technology infrastructure and emerging technologies such as blockchain and Internet of Things cause cyber threats. The threats target specially the assets of the banks, such as customer data and funds.

Keywords: cyber threat, banking sector, cybercrime, financial technology

TIIVISTELMÄ

Keränen, Annu-Maria
Pankkisektoria uhkaavat nousevat kyberuhat
Jyväskylä: Jyväskylän yliopisto, 2022, 34 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Mehtälä, Saana

Teknologian kehittyminen johtaa uusiin innovaatioihin niin yritysten liiketoiminnassa kuin jokapäiväisessä elämässäkin. Teknologian kehittyessä kehittyvät myös kyberuhat. Pankkisektori kuuluu yhteiskunnan kriittiseen infrastruktuuriin, joten sen vakaudesta ja turvallisuudesta on pidettävä huolta. Pankkisektoriin kohdistuvia kyberuhkia on tutkittava, jotta luottamus rahoitusjärjestelmään säilyisi vahvana. Tämän kirjallisuuskatsauksena toteutetun tutkielman tavoitteena oli määritellä pankkien kohtaamat kyberuhat sekä niiden kehittyminen tulevaisuudessa. Tutkielmassa tarkasteltiin pankkien toimintoja, jotka ovat erityisen alttiita kyberuhille ja teknologioita, joita pankit hyödyntävät. Tämän jälkeen käytiin läpi pankkisektoriin kohdistuvia kyberuhkia sekä niiden kehitystä. Tutkielmassa tarkasteltiin myös koko ajan kasvavaa finanssiteknologia-alaa ja sen aiheuttamia uhkia. Tutkielma perustui pankkien kyberturvallisuudesta, pankkisektorista sekä finanssiteknologiasta aiemmin tehtyihin tutkimuksiin. Pankkien kohtaamista kyberuhista tutkielmassa nousivat esiin erityisesti kyberrikollisuuden muodostamat uhat sekä organisaation sisältä tulevat uhat. Näiden lisäksi kyberuhkia aiheuttavat heikkoudet informaatioteknologian infrastruktuurissa sekä kehittyvät teknologiat, kuten lohkoketjut ja esineiden internet. Uhat kohdistuvat erityisesti pankkien omaisuuteen, kuten asiakkaiden tietoihin sekä rahavaroihin.

Asiasanat: kyberuhka, pankkisektori, kyberrikollisuus, finanssiteknologia

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

This bachelor’s thesis studies cyber threats that target the banking sector. The aim of the thesis is to find out which banking operations are especially under threat, what are the cyber threats that target the banks, and how evolving technology affects the development of these cyber threats. Cyber threats are evolving almost synchronously with technology (Li, 2017) and cybercrime acts are increasing and becoming more severe (Lallie et al., 2021). This requires continuous development of technical capabilities and resources from banks to be able to manage these threats (Blauner, 2013). Cybercriminal activities have already led to many costly cases, and measures to defend banking operations from cyber threats can cost millions (Carin, 2017). Cyber threats targeting the banking sector can undermine the stability and trust in the banking system and even cause cross border consequences (Carin, 2017), meaning that realized cyber threats can have major effects on the economy and societies. Because of the severe consequences that cyber threats can cause, it is important to study this issue and contribute to the research that enables the banking sector to develop more resilient against rising threats. This research can be utilized as a preliminary guideline throughout the banking sector when determining the cyber threat landscape and designing defense protocols in banks. Based on previous literature about cybersecurity and the banking sector, this thesis aims to discuss cyber threats that are characteristic of the banking sector and how the threats are evolving by answering research question:

- What kind of cyber threats is the banking sector facing in the near future?

To help to form the base for the research question, this thesis also examines how cyber threats, especially cybercrime, affect banks and banking operations and which of these operations are prone to cyber threats. This thesis also studies which technologies are utilized, and which new, emerging technologies are expected to become more common in the banking industry. In addition, the vulnerabilities that technological solutions include and the current threats that have the potential to benefit from technological advancement are discussed.

The financial sector, including banking sector, is a part of society's critical infrastructure (Blauner, 2013). Reliable banking operations are a prerequisite for financial stability and economic growth (Haw, Ho, Hu & Wu, 2010). Barone (2021) describes banks as financial institutions that have a license to receive deposits and make loans. These institutions can also provide other financial services, such as wealth management, currency exchange, and safe deposit boxes. The banking sector includes different kinds of banks, such as retail banks, commercial or corporate banks, and investment banks. Banks provide essential services to individuals and businesses, making them a crucial part of society. (Barone, 2021.) Digitalization has enabled new solutions for banking operations to rise and forced traditional banks to evolve. One of these solutions is financial technology (FinTech). IMF/World Bank Bali Fintech Agenda (2020) defines FinTech as advances in technology that can change financial services delivery methods and encourage new business models, applications, processes, and products. FinTech covers for example cryptocurrencies and the use of artificial intelligence for fraud detection, in addition to innovation in more traditional financial services. (Baba et al., 2020.)

According to the National Institute of Standards and Technology by U.S. Department of Commerce (2012), a cyber threat is any circumstance or event with the potential to impact individuals, organizations, or nations through an information system using unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Cyber threat can also be defined utilizing the CIA model of information security. The CIA model is a triad which consists of three characteristics of security: confidentiality, integrity, and availability. As Warkentin and Orgeron (2020) present, confidentiality means protecting data from unauthorized access, integrity refers to protecting data validity against unauthorized changes, and availability stands for the accessibility of information and systems to authorized individuals and processes. Canadian Centre for Cyber Security (2021) defines cyber threat using the CIA model as an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains. Some examples of cyber threats towards banking operations include data manipulation and theft, malware as a service as well as threats posed by blockchain, Internet of Things, and artificial intelligence (Creado & Ramteke, 2020). The term cybercrime has different definitions in literature depending on the writer's perspective, but it can be defined as an act that violates the law and is executed using information and communication technology to facilitate a crime or to target networks, systems, data, websites, and/or technology (Smith & Stamatakis, 2020). Cybercrime can be for example spreading virus programs, hacking and cracking, spam emails, phishing, and obtaining unauthorized access to other computers in order to steal something (Ali, 2019). Cyber-attack refers to an attack that is launched from one or several computers against other computers or networks, with the goal of disabling them or gaining an access to them (Carporale, Kang, Spagnolo F. & Spagnolo N., 2020).

Previous literature of cyber threats in the banking sector often focuses on a specific region. Literature on the banking sector's cybersecurity focuses mostly on the legal aspect of cybercrime as well as cybersecurity regulation. Many articles about cybersecurity in the financial industry cover the whole financial sector and give a more generic view of cybersecurity in the field. This thesis aims to find the most relevant threats specific to the banking sector. The goal is to build a comprehensive view of the threat landscape that targets the banks.

This research was conducted as a narrative literature review, as explained in Templier and Paré (2015). Preliminary literature was selected based on the relevance and topicality of the research, meaning that old articles and articles with no financial sector focus were excluded, with a few exceptions regarding some of the concepts, case examples, and technological specifications. Literature selection focused on recent articles because technology develops rather quickly, yet some older articles were utilized in finding out the development of cybercrime and certain technologies. The literature was selected based on searches on JYKDOK of peer reviewed international e-materials using the search terms "cyber threat", "cybercrime", "bank", "banking sector", "banking operation", and combinations of these. The same terms were used in Google Scholar searches as well. Only articles that were available in English were used to avoid misinterpretations in translations. For example, Google Scholar gave 1 590 results from English pages with the search term "cyber threat" AND "bank" with the timeline being set from 2015 to 2022. Using the same search term and timeline in JYKDOK's international e-material search gave 6 902 English, peer-reviewed articles, where full text was available. Because of the vagueness of the search terms and the extent of the subject, most of the results were not relevant. After selecting the preliminary literature, more precise search terms, such as "insider threat", "social engineering", "fintech AND cyber threat", and "future of banking", were used to find more specific literature. Multiple databases were used to find accurate materials from both disciplines, such as Scopus, Wiley Online Library, Emerald Insight, and IEEEXplore in addition to JYKDOK and Google Scholar. Additionally, the snowballing technique was used to find further materials from the references of the search results. Results that could not be entirely accessed due to paywall or missing full text were excluded from the research. Collected research was evaluated either by using Jufo-rating or by reviewing the editorial policies, impact factor if available, and peer review process of the publication. Some unscientific references, such as relevant websites and reports, were used in definitions and case examples. The reports were used to highlight current cyber threats and incidents that have not yet been scientifically researched.

As a result of this research, it was found that the most relevant cyber threats that must specifically be noted by banking institutions are cybercrime actions and vulnerability of data. The results suggest that current banking operations as well as future operations utilizing emerging technologies pose as a threat especially to the security of customer data and assets. As data quantities increase with new technological improvements that can collect and store massive amounts of data, its value also increases, and it becomes a target of cybercriminals. Emerging technologies offer a variety of data protection systems and tend to be more secure, but as humans are behind the technological advancement, humans can also be able to break into the systems. This results in technological solutions never being completely secure and the continuing existence of cyber threats. Banks utilize third party service providers and most likely will continue to do so in the future, which maintains the cyber threats related to those.

This research consists of introduction, two chapters, and a conclusion. The next chapter reviews banking operations that are under threat and presents the cyber threats that target the banking sector. The third chapter discusses the future of the banking sector and how it affects cyber threats, as well as answers the research question. The thesis is concluded in the last chapter, which summarizes the motivation behind this thesis, the utilized research method, and findings of the research.

2 CYBER THREATS TARGETING THE BANKING SECTOR

This chapter reviews which banking operations are prone to threats and what are the cyber threats that the banking sector is facing. The use of information technology has spread wide in the banking industry, which increases cyber threats because cybercriminals can exploit the system vulnerabilities and different types of innovative crimes can occur unexpectedly. Cyber threats are unpredictable and continuously changing, which affects the growth and finances of the banking sector. (Uddin, Hakim & Hassan, 2020.)

Most cyber threats are caused by humans. Human error or negligence is behind a notable portion of data breaches (Farshadkhah, Van Slyke & Fuller, 2021). A system loophole can be exploited by a human with malicious intentions, or a human can plan and execute a cyber-attack on an institution with the goal of gaining financial profit. Cybercriminals often have different motives, which include financial gain, espionage, or coercion (Lallie et al., 2021). While all of these make the banking sector an enticing target for attackers, banking sector is usually targeted by financially motivated cyber threat actors (Noor, Anwar, Amjad & Choo, 2019).

2.1 Banking operations under threat

The European Central Bank (ECB) states that digitalization brings risks to the payment system, to monetary sovereignty, and the whole financial system (ECB, 2021b), including the banking sector. According to Uddin et al. (2020), cyber threats affect financial institutions' earnings, business growths, and overall business risks. Cyber threats can lead to direct and indirect financial losses, but also loss of the customer confidence. For example, a hacked financial institution can suffer losses related to opportunity costs for service breakdown, costs for incidence detection and cleaning up the aftermath of cybercrime, costs associated with the loss of confidential business information and intellectual property, and loss of reputational damage. (Uddin et al., 2020.) Therefore, the costs of cyber threats can get colossal.

Banks perform activities, of which some are mandated by law, and some are voluntary. These activities are called banking operations. Most of banking operations are nowadays virtual which makes it essential to ensure the integrity and confidentiality of information (Uddin et al., 2020). Operations that are vulnerable to cyber threats include for example online banking activities and electronic financial transactions (Ali, 2019). Vulnerable systems include peer-to-peer transactions, producing sentiment analysis, digital currencies, and Society for Worldwide Interbank Financial Telecommunication (SWIFT) -based transaction systems (Creado & Ramteke, 2020). Banks collect, store, and handle a huge quantity of confidential data, which is a tempting target for cybercriminals because of its value. For example, if an attacker stole data such as credit card and bank account numbers or personal information, this information could be traded on a black market (Wang, Gupta & Rao, 2015). An example of a disastrous cyber-attack is the attack on Pakistan's banking system in 2018, when hackers stole bank-issued cards from bank Islami and sold them on the Dark Web. The data of almost 20,000 cards was compromised in the cyber-attack which affected the whole payment network and international payment scheme of bank Islami. (Khan, Mubarik & Naghavi, 2021.) Cyber threats risking the data of banks can reduce the stability and trust in the financial system (Carin, 2017). Fund transfers between banks can be prevented, confidential data can get stolen and operations of other sectors that rely on integrated banking services can be damaged by hackers (Uddin et al., 2020).

2.2 Cyber threats targeting the banks

As Uddin et al. (2020) state, cyber threats are unpredictable, as no technology can foresee when and how an incident will occur. Technology use in banking operations and services delivery is high, which means that banks are exposed to the unremovable systematic risk of technology. Systematic risk means that a single breach in a banking network can upset the whole financial system because of the interconnectedness of banks and financial institutions. Technical faults, like system failure and program errors are always a threat within virtual environments, in which most institutions operate this day. Technology can never be completely secure, which creates an opportunity for criminals to infiltrate into the systems. (Uddin, et al., 2020.)

Internet of Things (IoT) offers a source of vulnerability. An increasing number of devices are connected to the internet, and they are not often secure enough, which exposes them to malicious behavior (Carin, 2017). Ye, Cao, and Chen (2020) present that IoT security consists of securing connected networks and devices. Main IoT security issues that can inflict security breaks are default and hardcoded passwords, linking a legacy asset that is not intended for IoT network, the lack of industry-acknowledged guidelines as well as the fact that

IoT devices often do not have resources to ensure high enough security. In IoT systems, data exchange and information verification are performed over the central server, which also creates privacy and security concerns such as false authentication, lower reliability, and device spoofing in data sharing. (Ye et al., 2020.) The network of these cyber-physical systems can be devastating if an intruder with malicious intentions gets access to supervisory control (Khan et al., 2021).

Weakness in digital infrastructure, vulnerable operation systems, and service versions are common cyber threats (Carin, 2017). Vulnerability in operating system enables hackers to exploit the system and cause both direct and indirect losses for the breached institution. Regardless of technological sophistication, some unknown loopholes tend to exist in systems which makes a cyber breach often unavoidable. (Uddin et al., 2020.) Uddin et al. (2020) suggest that cybersecurity providers might leave flaws in systems because software development monitoring is not regulated, and ethical standards of programmers are not upgraded and maintained. An example of these loopholes is the cyber heist that targeted the central bank of Bangladesh. The U.S. federal reserve released 81 million dollars to hackers who sent fake SWIFT messages in disguise with the goal of transferring money from the Bangladesh Bank's account. Anyone infiltrating a network, in which two devices are connected in, can send a false message in disguise. This was the case in Bangladesh bank's heist. The system vulnerability should be properly secured at the institution level to prevent the impact of this kind of cyber breach from spreading over all financial institutions in the processing chain. (Uddin et al., 2020.)

In addition to cyber threats resulting from criminal activities, cyber threats can also be caused by natural disasters or other major events (Sailio, Latvala & Szanto, 2020). Natural disasters can for example destroy a data center, but also cybercriminals can take advantage of them. The infrastructure and people being in a vulnerable state because of natural causes makes them an easy target. The cybercriminal activities that can be used also during natural disasters are discussed in the next chapter.

2.2.1 Threats posed by cybercrime

Financial sector is the main target of cybercriminals and several of the offenses against financial institutions are large-scale breaches, frauds, and heists (Uddin et al., 2020). Das (2019) highlights that also organized crime has realized the possibilities of financial cybercrime against banking institutions, as it is profitable with less risk of getting caught than traditional crime. The author also mentions that state-sponsored hacking against financial institutions should not be underestimated, as state-organized actors form an active cyber threat (Das, 2019). Cybercrime can easily have cross-border consequences because of internet vulnerabilities and inadequate security (Carin, 2017). Cybercrime can affect the growth of the banking sector, so threat management is needed to maintain sustainable business growth and secure financial business environment (Ali, 2019). The banking sector has seen many costly instances of denial of service (DoS), ransomware, and hacking. Breaches in the industry are widely reported and credential theft, malware currency manipulation, and disk-wiping attacks require massive investments from banks to defend themselves. (Carin, 2017.) According to Ali (2019) many of the banks in the region of Gulf Countries Council only request username and password to access online banking services which poses a serious threat to a bank's security system, as it makes it easy for cybercriminals to get a hold on user's account. European Central Bank's newsletter in 2021 revealed that the most frequent cyber incident at banks in 2020 were distributed denial of service (DDoS) attacks. Later that year a variant arose in which the perpetrators threatened banks with a DDoS attack unless a ransom was paid. In 2020 also emerged an elaborate cyber-attack in which a common monitoring software was manipulated. This caused organizations to download a piece of malware during the software's normal updating process without knowing. Other cyber incidents in 2020 reported by ECB were denial of service attacks, malicious script injections, ransomware, trojan horses, brute force attacks, mobile malware, viruses and worms, accidental data leakages or corruption, insider or third-party threats, and social engineering incidents such as pretexting, phishing, and spear phishing. (ECB, 2021a.) Typical cyber-attacks against IoT systems are for example incorrect signal injection, spoofing, eavesdropping, and replay attacks. These types of attacks compromise user data, which is often private information and therefore form a serious security threat. (Ye et al., 2020.)

Hacking compromises the confidentiality or integrity of a system. Hacking requires technical expertise as its techniques include for example exploiting system vulnerabilities to break into the system. (Lallie et al., 2021.) For example, hacking was used when an intruder planted the Zeus Trojan Horse virus into a computer of the State Bank of Bellingham. The virus permitted access to the computer and the intruder was able to make unauthorized money transfers to other banks. (Weissman, 2017.) Malware refers to malicious software and it can be used to disrupt services, extract data, or other actions. Most common type of malware today is ransomware, in which malware is combined with extortion attempts. DoS attacks target system availability by flooding main services with illegitimate requests and the goal is to force the server offline by consuming the bandwidth used for legitimate service requests. (Lallie et al., 2021.) Intentional information technology system failure or breakdown, such as DDoS attack, allows criminals to inject the banking system with malware or other spyware, since they may shut down banking services completely (Uddin et al., 2020). Another instance of cybercrime is Emotet, which is one of the most professional and long-term cybercrime services. Emotet was first discovered as a banking Trojan in 2014, and subsequently developed into a multipurpose door-opener for different computer systems, enabling further illegal activities. (Europol, 2021a.)

2.2.2 Threats from within

Threats that originate from sources that are within the organization are called insider threats. Insider refers to an employee or other who has access privileges and knowledge of organization's internal processes. The threat an organizational insider poses is significant and growing, because even one malicious employee inflicting a breach can be destructive. (Willison & Warkentin, 2013.) Financial institutions depend on information technologies and store sensitive data which makes them particularly vulnerable to insider threats (Wang et al., 2015).

According to Willison and Warkentin (2013), insider threats can be divided into three levels. Firstly, insider threat can be passive and non-volitional, meaning that a violation that an employee makes is not intended. For example, an employee might accidentally entry incorrect data values which can threaten data integrity. Insider threat can also be volitional but not motivated by malicious intentions, meaning that an employee chooses to violate security policies, but not with the intent of causing harm to the organization. This behavior can cause damage or a security risk. These choices can be for example delaying data backup, failing to encrypt data before transmitting it, or failing to secure a private space to discuss sensitive information with a customer. The third level of insider threat is malicious computer abuse by insider, which means intentional behavior with malicious intentions. This can include for example data manipulation or destruction, data theft, fraud, blackmail, embezzlement, stealing credit card numbers, and disclosing confidential information. (Willison & Warkentin, 2013.)

Cybercrime can target technology but also human aspects (Lallie et al., 2021), of which one instance is social engineering attacks. Social engineering activities result in unintentional insider threats, as they often target employees of an organization (Klimburg-Witjes & Wentland, 2021). According to Lallie et al. (2021) the term social engineering is used to describe a situation where an illegitimate party tries to convince an individual to perform an action in the belief that they are engaging with a legitimate party. These actions can be for example sharing information or visiting a website, and the target can be contacted via email, text message, or other similar way. Deceiving individuals or organizations using technology is a common way for an attacker to gain financial profits. Social engineering can include extortion, where individuals or organizations are forced, threatened, or coerced to perform actions, usually releasing finances. (Lallie et al., 2021.)

Social engineering is a psychological manipulation technique used to profit from other's disadvantage. According to Ghafir et al. (2018b), the most commonly recognized social engineering attack model is Kevin Mitnick's social engineering attack cycle (2002). It consists of four stages, which are research, develop rapport and trust, exploit trust, and utilize information. Research stage consists of gathering useful information about the target. In the second stage the attacker aims to gain trust of the target, which is then exploited in the third stage to induce information from the target, manipulate the target, or instruct the target to implement actions. The final act of attack is utilizing information that was acquired in the first three stages to get to the wanted result. (Ghafir et al., 2018b.) Social engineering is the most common way of intruding and infecting computer systems and information technology infrastructures today (Klimburg-Witjes & Wentland, 2021). Social engineering attacks include for example pre-texting, phishing, spear phishing, and vishing. These attacks can lead to users of a bank's system releasing confidential data (Uddin et al., 2020). Attacks can also be used to spread malware or to steal the identity and information of banks' customers to use banking services and withdraw funds (Khan et al., 2021). In case a social engineering attacker manages to steal for example a bank manager's confidential personal identification number, the banking system may face serious fraudulent transactions (Uddin et al., 2020). Social engineering attack can be for example using phishing method to distribute malware, with the objective to steal payment credentials from a compromised system (Lallie et al., 2021).

Intentional insider threats include intentional misuse of access rights and human abuse of technology (Uddin et al., 2020). One major insider threat is unauthorized access attempts on information systems applications, as they are widely used to support business operations and to store data. These attempts often lead to system breach and data loss. (Wang et al., 2015.) Attacks caused by malicious insiders are often harder to detect than attacks coming from outside the organization (Homoliak, Toffalini, Guarnizo, Elovici & Ochoa, 2019), which stresses the seriousness of insider threats. Homoliak et al. (2019) present some of the intentional insider attack types, which include misuse of access, where an insider uses a legitimate access for improper purpose, defense bypass, where an insider passes defense, such as firewalls, and access control failure, where access control element has vulnerabilities or the element is misconfigured, which allows the insider to get access. Malicious insiders might use information technology to cause specific harm to an organization or to modify, add, or delete organization's data for personal gains or to damage, destroy, or sell out their organization. Insiders might also steal intellectual property of an organization to use it for their own business, take it to a new employer, or pass to another organization. (Homoliak et al., 2019.)

According to Giacchero and Moretti (2021), financial institutions use third-party service providers to employ solutions that are not available within the institution. These vendors form a third-party threat since a cyber-attack on them compromises the data of their customers. Third-party threats regarding information and communication technology providers are a concern to all financial institutions because outsourcing technology services is common in today's banking. These external services can be for example software development and maintenance, network and server management, and applications. Third-party service providers are prone to cyber threats alike banks themselves. Main concerns are security threats, such as data leakage and cyber-attacks. (Giacchero & Moretti, 2021.) For example, banks may use third-party vendors to handle their security systems, which means that they may have access to all confidential data of the institution (Uddin et al., 2020). A cyber-attack that compromises the data of the third-party vendor also threatens the involved bank.

3 FUTURE OF CYBER THREATS IN THE BANKING SECTOR

This chapter discusses the future of banking operations as technology evolves as well as the cyber threats that develop due to it. Lastly, the results of the research are summarized. The use of digital technologies in banking operations has increased cyber threats. Cyber-attacks have become more sophisticated (Lallie et al., 2021) and this development is not expected to stop. The fact that cybercrime is becoming more frequent and severe (Lallie et al., 2021) signals that the threat of cybercrime is here to stay. Cybercriminals do not only target individual banks, but also spy on other sectors to get important business information that is indirectly linked to the banking sector. Even though the banking sector has emphasized different technological security methods, the protection infrastructure will always be vulnerable, partly because of increasing cybercrime. (Khan et al., 2021.)

3.1 Future of the banking sector

Digitalization has changed and is likely to continue changing the way banks operate. Broby (2021) presented that the use of internet has changed the way banks perform their functions such as payments and transfers, how transactions are recorded on ledgers, and how private and public digital currencies are facilitated. In the future, banks must access deposits and process transactions made in digital form, either Central Bank Digital Currencies or cryptocurrencies, which requires actions by banks to maintain resilience and security. Progress in technology allows digital money to be cryptographically protected and the use of cryptocurrencies is increasing as a digital wallet fulfills mostly the same storage and transmission operations as banks. (Broby, 2021.) Banking operations are impacted by unintentional system breakdowns as well as intentional breaches. The worst-case scenario is that these incidents affect the whole banking network. Continuous technological upgrades, improvements in software and hardware, as well as information technology training and human development require ongoing investments from banks. (Uddin et al., 2020.)

3.1.1 Financial Technology

Financial technology is noted as one of the most important innovations in the financial industry and it is evolving and spreading quickly (Gang, Özlem, Hasan & Serhat, 2021). FinTech is facilitating banking as a service by delivering services over the internet without turning to the balance sheet (Broby, 2021). Its purpose is to apply information technology -based service solutions to increase efficiency in banking transactions and financial markets (Palmié, Wincent, Parida & Caglar, 2020). FinTech investments can for example enhance money transferring and savings systems (Gang et al., 2021). Palmié et al. (2020) suggest that FinTech is a new domain for banking industry as FinTech companies provide alternative banking solutions such as digital lending, personal finance, online and mobile banking, peer-to-peer lending, and investment management. Financial technology has benefited from technological advancements in online payments, cryptocurrency, and artificial intelligence (Palmié et al., 2020) and it has automated for example credit evaluation, savings, investments, trading, banking payments, and risk management (Broby, 2021). However, the security of these operations depends highly on the technology on which they are built. (Broby, 2021).

According to International Monetary Fund Working Paper from 2020, cross-border and pan-euro area instruments have not yet spread widely but digital payment systems are expanding within countries. Large banks in European Union have adopted new technologies, such as cloud computing, mobile wallets, biometrics, and artificial intelligence. Banks are adapting to solutions which improve data security and authentication, such as one-time dynamic security codes, and biometric recognition technology instead of card numbers. (Baba et al., 2020.) New payment technologies still have cybersecurity concerns. Artificial intelligence and machine learning can be used to mine customer data inexpensively, but these can also bring threats regarding misuse and breach of customer privacy. Banks in the European Union have developed in-house technologies but also have commercial partnerships with external FinTech companies. (Baba et al., 2020.) These partnerships can create a third-party threat to the institution, as discussed in the second chapter.

Consumers are shifting their preferences to online and mobile banking, which forces banks to provide digital applications. This enforces the dependence of technology and strengthens the existence of cyber threats. Technology brings threats through security breaches and fraud during financial transactions. (Palmié et al., 2020.)

3.1.2 Open Banking

Open Banking is a new way of handling banking data protocols (Broby, 2021). It is a data sharing solution, in which the goal is to remove barriers to data access and increase customers' control over their data (Kellezi, Boegelund & Meng, 2021). It means that a bank can securely make direct payments and download financial data from a customer's banking website, to which the customer has given a regulated Application Programming Interface (API) permission through a third-party provider (Broby, 2021). To utilize Open Banking, banks have to develop APIs that provide access to bank account data and information as well as enable transactions between different accounts (Kellezi et al., 2021).

Although secure protocols and layered permission access are utilized, Open Banking still has some security and privacy concerns because the system requires banks to grant access of data to third payment service providers (Broby, 2021). Open Banking exposes data to more actors than banking solutions before because APIs can expose data to a third party. This means that existing security threats are increasing, and new threats are emerging. Using applications on a web platform, that might have insecure protocols, is also increasing the threat. Threats related to Open Banking APIs include injections, broken authentication, sensitive data exposure, broken access control, security misconfiguration, and insufficient logging and monitoring. Blockchain technology could be utilized in open banking systems to increase reliability and trust communication between users and third-party services. (Kellezi et al., 2021.)

3.1.3 Utilizing blockchain technology

Blockchain technology has been widely adopted in the banking industry and will likely continue to spread in the future because it reduces transaction costs and processes transactions faster than traditional banking products. Blockchain technology enables fast, cost-effective, and secure cross-border transfers of assets by utilizing peer-to-peer distributed networks and applying open-source cryptographic protocol. (Osmani, El-Haddadeh, Hindi, Janssen, Weerakkody, 2021.) Guo and Liang (2016) suggest that the use of blockchain can lead to reconstruction of the financial infrastructure and has the potential to become the underlying technology of the financial sector. However, to form a seamless distributed digital transaction process, conventional technology standards and protocols need to be employed (Osmani et al., 2021). Blockchain applications promote decentralized scenarios which are supposed to enhance the efficiency of banking operations. Complete decentralization might not be possible in the financial sector, because some operations need to be secured by centralization and intermediaries. Banking sector could however utilize a more centralized consortium and private blockchains instead of completely decentralized public blockchains. (Guo & Liang, 2016.)

Currently transactions in FinTech's setup take from a day to several days between issuance and settlement. Implementing blockchain to mediate transactions could improve performance so that the transactions could proceed in a fraction of that time. However, blockchain security is not yet up to FinTech requirements. (Eyal, 2017.) Some of the security challenges of blockchain technology will be addressed in the upcoming chapter.

3.2 How the threats evolve

The cyber threats that target the banking sector are especially cybercrime activities that target the vulnerabilities in information technology systems or the humans using them. The development of these threats is important to know and is an interest of not only the banking sector but also the cyber security industry. The key in being able to defend critical operations is the identification of the threats and the development of appropriate defense mechanisms. New technology is invented and deployed at a rapid pace which means that there is also room for new threats to arise. Not all these threats can be foreseen, as system vulnerabilities are often only detected as the breach occurs.

As previously stated, humans are usually cyber threat actors. Uddin et al. (2020) present that a human has a motive to deploy technology to reach their goal, which can be for example gaining profit or harming a business, when an opportunity to do so arises. Because the motives of humans are nearly impossible to control, the defense technologies used by banks should evolve and aim for higher security. This leads to technological dependence, where investments in technology are made but cyber threats still exist. (Uddin et al., 2020.)

As technology becomes more sophisticated and institutions' solutions to protect their assets are enhanced, cybercriminals will continue to exploit human weaknesses to achieve their objectives (Ghafir et al., 2018b). Social engineering is and will be an efficient way to do this. As humans are generally the weakest link in information security (Klimburg-Witjes & Wentland, 2021) the threat of social engineering is expected to continue in the future. Social engineering is a rapidly increasing threat and has potential to be catastrophic. It is an unavoidable threat, since all computer system users cannot be trained effectively, and attackers will always develop new ways to deceive even the most trained users. (Klimburg-Witjes & Wentland, 2021.)

The increasing technology use in banking sector offers a possibility for cyber threats to evolve and expand. Digitalization and the new banking solutions it brings result as increase in the quantity of data which might become even the most valuable asset for banks and therefore a target for cybercriminals.

3.2.1 Continuously evolving cybercrime

Because the banking sector is often the target for financially motivated cybercriminals, the future threats lay mostly in the hands of cybercriminals. Hence, it is relevant to examine how the criminal activities develop. It is important to notice that as new technologies are implemented, possibly to enhance security, the same technologies can be used to facilitate criminal activities. Europol (2021b) mentions that due to the increase in teleworking, the number of vulnerabilities and attack surfaces have risen. Cybercriminals can break into organizations' networks through remote desktop protocol connections and exploit vulnerabilities in virtual private network services (Europol, 2021b).

According to Europol's Internet Organized Crime Threat Assessment from 2021, crime-as-a-service (CaaS) business model is expanding. CaaS refers to criminal services, such as ransomware, being sold on the Dark Web (Europol, 2021b). Other criminal tools that are offered online include malware, phishing facilitators, sniffers, skimmers, and DDoS attacks (Europol, 2021a). Criminals are increasing their security by hiding their online activity, using more secure communication channels, and concealing the movement of illicit funds, which enables CaaS model to expand. With CaaS model enabling the availability of exploit kits and other criminal services, more criminals, even the ones with low technical expertise, have the possibility to execute sophisticated cyber-attacks. CaaS can also increase the efficiency of organized cybercrime. The development and specialization of CaaS enables more large-scale ransomware attacks, that cause even bigger losses to the organizations. Ransomware affiliate programs are increasing, and they are offered to a wide range of potential users on the Dark Web. Criminal groups are maturing, and they are searching for developers and hackers to improve the quality of their products. Criminal groups can also collaborate with each other, for example to develop and execute more advanced attacks. (Europol, 2021b.) Banking sector is the target of financial fraud, which can include stocks and securities investment fraud, SIM-swapping, and deepfakes. Methods for fraudulent investing activity are for example market manipulation, insider trading, money laundering, and terrorist financing. Deepfakes can be used for example in spoofing and manipulating employees of an organization. (Nicholls, Kuppa & Le-Khac, 2021.) Europol (2021a) states that criminal use of artificial intelligence, including the exploitation of deepfakes, is expected to increase in the future.

3.2.2 Threats from emerging technologies

Financial technology applications integrate several different technologies, such as embedded systems, mobile computing, cloud, big data, data analysis technology, and embedded cloud computing (Meng, He & Tian, 2021). In addition, machine learning and deep learning methods are used in the banking sector to support operations and provide cybersecurity (Nicholls et al., 2021). FinTech's main issues are related to security and privacy, as well as authentication and access control mechanisms. Main concerns about security and privacy are how to protect sensitive data and how to carry out secure electronic transactions. Data protection mechanisms are important to ensure secure access to data, but they are usually complicated to implement and adjust. (Meng et al., 2021.) FinTech industry is especially vulnerable to data breach that use advanced persistent threats (APTs). APTs are increasingly sophisticated and create a severe cyber threat against banks and FinTech companies. (Noor et al., 2019.) According to Ghafir et al. (2018a), the APT attack is a persistent, targeted attack which is executed through several steps. APTs use advanced techniques and utilize unknown vulnerabilities with the main objective of espionage and data exfiltration (Ghafir et al., 2018a). APTs are becoming more common, and they can lead to massive losses. For example, a FinTech company Equifax was compromised in an APT incident which resulted in 148 million customers having their personal information and credit card credentials accessed. (Noor et al., 2019.)

Banks have adopted technologies like Internet of Things (IoT), big data analytics, and cloud computing for financial services because of not only their ability to store great amounts of customer data, but also banks' need to improve data sourcing and insight creation from data. For example, using IoT in automated teller machines helps customers to access their money easily without payment cards, but also allows banks to collect, exchange, and create insight from each transaction. (Abeeku, Agoyi & Agozie, 2021.) According to Padmaja and Seshadri (2019), cloud systems are highly adaptable which makes it easy for banks to migrate to them. The use of cloud systems can also be beneficial to banks as it reduces management and infrastructure costs and enables banks to perform globally. However, information in the cloud is usually sensitive and cloud systems are known to have security issues. One major threat is that a data breach results in sensitive information exposing to an unauthorized party. Other considerable security issues in addition to data leaks are loss of intellectual property, data privacy, and system security. Cyber-attacks targeted at cloud systems are usually denial of service and phishing attacks, and they typically result in information lockout and application unavailability. These security attacks usually lead to service down time, unavailability of services, and breach of data privacy. (Padmaja & Seshadri, 2019.)

Abeeku et al. (2021) present that the use of virtual cloud computing, used by approximately 89% of banks globally, supports the IoT and big data analytics. However, these applications are complex and network connectivity for data transmission and storage via the Internet results in continuous threats and vulnerabilities. Institutions become more and more prone to cyber threats as they depend on emerging digital innovations. Integrated IoT, big data analytics, and cloud computing infrastructures are targets for hackers. Lack of security requirements on these integrated platforms compromises the security of data and information. Integrating IoT, big data analytics, and cloud computing can create threats related to access control vulnerabilities, network security attacks, data and information management vulnerabilities, infrastructure attacks, security and identity management failures, and communication security failures. Identity management and access control failures expose the system to identity theft, altered privileges, and attacks if IoT nodes fail to authenticate authorized access on a cloud platform. Threats like DoS and DDoS attacks as well as spoofing and phishing affect especially IoT devices that transmit data and information through the cloud platform. Integrated IoT, big data analytics, and cloud computing platforms are also challenging for data management. Threats following data management challenges are for example failure to secure data transferability, failure to provide data privacy, lack of data prevention, and failure to prevent unauthorized access. (Abeeku et al., 2021.)

Cloud computing also raises insider threats. Malicious insider can be for example an unsafe cloud provider administrator, who can access data or other resources, insider who exploits cloud vulnerabilities for unauthorized purposes, or insider who exploits the cloud services to perform criminal activities against the organization. These malicious insiders might leak or misuse data, perform DDoS attacks against the organization, or crack password files. (Homoliak et al., 2019). Cloud computing providers are usually not subject to the regulation of the financial sector authorities, which enhances the existing third-party threat. (Giacchero & Moretti, 2021.)

3.2.3 Blockchain technology vulnerabilities

According to Osmani et al. (2021), using new technologies such as blockchain in banking operations enhances inter alia operational risks. Operational risk means potential losses resulting from significant deficiencies in system reliability and integrity. These deficiencies can be for example hardware or software failures, disruptions, or database compromise. Operational risk arises mainly from cyber-attacks, where attacker obtains confidential information by manipulating data or altering account balances. (Osmani et al., 2021.)

Even though some aspects of blockchain technology improve the security of transactions and data, it is still vulnerable to cyber-attacks. For example, the attack on the Ethereum blockchain cleared about $50 million from a so-called decentralized autonomic organization. The attacker managed to withdraw funds repeatedly after using a recursive property of the Ethereum programming language to withdraw funds without having the withdrawal accounted for. (Eyal, 2017.) Blockchain systems are prone to security and data integrity attacks. These attacks include majority manipulation, consensus delay due to DDoS, selfish mining, pollution log, blockchain forking, orphaned blocks, de-anonymization, block ingestion, double spending attacks, and liveness attacks. In the majority manipulation attack, where a miner's hashing control is over 50% of the entire hashing control of the whole blockchain, the information on blockchain can be manipulated and modified. (Bhutta et al., 2021.) For example, the security in Bitcoin's blockchain system is based on a longest-chain rule. If an attacker succeeds to form a longer chain than the main chain, all other miners will switch to the attacker's branch. This kind of attack can succeed if the attacker's computational power is more than of the legitimate miners. (Eyal, 2017.)

Dong, Luo and Liang (2018) mention that blockchain creates excess information as individual nodes participate in the verification process of each transaction, which consumes more power and takes additional storage. In addition, a targeted cyber-attack on one node enables the attacker to understand the whole network's dynamic information. It is likely that viruses and attacks targeted at blockchain leveraging systems will emerge in the future. Also, smart contracts established by blockchain are vulnerable to exploiting attempts since they may contain design flaws and bugs and usually deal with valuable digital assets directly. (Dong, Luo & Liang, 2018.) These bugs in smart contracts cannot be directly fixed because of the immutability of blockchain (Bhutta et al., 2021).

Other vulnerabilities of blockchain are third-party and privacy threats. Banks might not want a third party to be able to track transactions for the sake of their competitiveness and customers' privacy. Self-generated cryptographic keys that are used in blockchain technologies as an identification do not reliably ensure privacy. Mixing funds to obtain privacy is vulnerable to DoS attacks in which one participant prevents the construction of the transaction. (Eyal, 2017.) A user's account might get tampered with if the user's private key gets in the wrong hands. In addition, a public key can be used to browse previous transactions on the blockchain and all transactions related to that specific key, if the key has been linked with a person's identity. (Bhutta et al., 2021.)

Blockchain applications may include some transaction verification problems. Bootstrapping procedure can be used to verify block and transaction correctness, but if the data used for the procedure is not destroyed after bootstrapping, an attacker can use it to generate and reuse coins unnoticeably. (Eyal, 2017.) One weakness of blockchain is the double spending problem, where a user could use the same single digital token multiple times. An invader might utilize the intermediary period between double transaction's launch, by getting the output of the initial transaction before the subsequent operation has been mined as null. (Bhutta et al., 2021.)

Current vulnerabilities of blockchain technology are likely to pose as cyber threats also in the future because the development and diffusion of blockchain are still at preliminary stage. Security threats that blockchain poses are for example identity theft, hackers, and money laundering, as the blockchain provides transaction pseudonymity. (Gan, Lau & Hong, 2021.)

3.3 Results of the research

The previous chapters presented emerging technologies relevant to the banking sector and banking operations as well as possible cyber threats related to them. Cyber threats look mostly the same in the near future as today, with the addition that cyber-attack surfaces will increase with growing number of applications and connected devices. Operational risks, that come with increasing use of technology, are likely to form even bigger threat. In addition, cybercrime develops at the same pace with security methods and cybercriminals improve their methods and techniques to perform and offer even more advanced cyber-attacks and services. The possible future cyber threats found in this research are summarized in the table below (table 1).

TABLE 1 Future cyber threats

	Target	**Threat**	
		Internal actor	**External actor**
General threats	IT users	Disregard for security policies	Social engineering
	The whole banking sector	Passive & non-volitional and volitional & not malicious insider threats, malicious computer abuse, operational risks	Financial fraud, CaaS, third-party threat
Technology-specific threats	Blockchain	Transaction verification problems, security & privacy vulnerabilities	Majority manipulation, DDoS, selfish mining, pollution log, forking, orphaned blocks, de-anonymization, block ingestion, double spending attacks, liveness attacks
	FinTech	Vulnerabilities in access control	APTs, DDoS, phishing, fraud during financial transaction
	Integrated infrastructures	Access control and data management vulnerabilities, security failures	(D)DoS, spoofing, network attacks
	Open Banking	Broken authentication and access control, security misconfiguration, insufficient logging and monitoring, insecure protocols on web platforms	Injections, third-party threat

Teleworking and an increasing number of IoT devices, computer systems, and applications widen the attack surface for cybercriminals. Development of CaaS business model enables cybercriminals with less technical capabilities perform sophisticated attacks and makes the operations of criminal groups more profitable, as they can sell their services online. The use of classic cyber-attacks, such as DDoS attacks, trojans, ransomware, and other malware, seems to continue. However, to be able to get around evolving security controls, cybercriminals have to actively adjust their methods and techniques. For most cybercriminals targeting the banking sector the motivation is financial. With the quantity and value of data increasing, the aim in stealing data from an organization is to attempt to monetize it by, for example, blackmailing the organization and its customers.

Applications that work on web platforms, such as cloud systems, are continuously under cyber threats. Insecure protocols increase the threats related to web platforms. Data transmission and storage via the Internet makes systems vulnerable to cyber-attacks that compromise the security of data and information. FinTech is especially vulnerable to APTs, which can result in data breach, data extraction, and espionage. Open banking applications are vulnerable to injections, broken authentication, sensitive data exposure, broken access control, security misconfiguration, and insufficient logging and monitoring. Integrated applications have multiple vulnerabilities, such as access control and data management vulnerabilities, network security and infrastructure attacks, as well as security and identity management, and communication security failures. Blockchain technology-based applications are vulnerable to cyber-attacks in addition to privacy and verification problems. All these threats can lead to data leaks, where sensitive information is exposed to unauthorized party and intellectual property is lost. In addition, cyber-attacks can lead to information lockout and application unavailability.

As banks implement new technologies that automate operations, the possibility of human error in those operations decrease. Still, the insider threat exists because social engineering is an efficient way to exploit the weakest link in cybersecurity. Cybercriminals are inventing new ways and improving the old techniques to trick employees to get to their goal. Malicious insiders can expose an institution to major losses also in the future.

Banks collaborating with external FinTech companies increase the third-party threat. Third-party threat includes data security and customer privacy concerns. Open banking is one of the platforms where access to customer data needs to be granted by banks to a third-party. Also cloud systems include third-party threats. It can be an unsafe cloud provider administrator, insider who exploits cloud vulnerabilities for unauthorized purposes, or insider who exploits the cloud services to perform criminal activities against the organization. In addition, cloud computing providers, alike other FinTech companies, are usually not subject to the regulation of the financial sector authorities.

4 CONCLUSION

This thesis examined the cyber threats that target the banking sector, technologies that banks are adopting, and the future of the banking sector. The goal of this paper was to define the cyber threat landscape targeting the banking sector and examine the possible future threats. The intention was to compile all the relevant cyber threats that target the banking sector and clarify the possible future changes. To do this, multiple studies were used to find out the current threats and how they might evolve in the future, as well as how digitalization affects the banking operations in the future. This research was conducted as a narrative literature review which aims to combine scattered articles on a topic and provide a narrative summary of knowledge in a certain area (Templier & Paré, 2015). Preliminary literature for this thesis was selected mostly based on the relevance of the research's abstract because the initial keywords resulted in a large number of search results. Because of that, the collecting process was not systematic, and some relevant articles may have remained unnoticed.

The first chapter offered an explanation to why it is important to increase knowledge of the subject and gave definitions to relevant concepts. In addition, the research question was introduced. The banking sector provides critical services for society to function properly. Crisis in the banking industry can lead to crisis in every other sector of business and everyday life. The digitalization of banking industry has increased cyber threats. Cyber threats targeting the banking sector are significant because they affect the assets, reputation, and reliability of the banks. The effects of a cyberbreach have the potential to be catastrophic, as they might spread even globally.

The second chapter presented the banking operations that are vulnerable to cyber threats and the threats that target these operations. Banking operations today are mostly virtual, which makes them prone to cyber threats. Relevant cyber threats in the banking sector include cybercrime actions as well as insider threats and vulnerabilities in information technology systems.

The third chapter covered the future of banking sector and the threat landscape regarding emerging technologies. This chapter aimed to answer to the research question. It was found that the banking sector is moving towards new applications and solutions rapidly. Emerging technologies such as blockchain and cloud computing offer a wide variety of novel service solutions, but not without safety concerns. The main cyber threats regarding new technologies are data security vulnerabilities and cyber-attacks. As new technologies increase the amount of data, its value rises, and it becomes a more profitable target for cybercriminals. The importance of secure handling of data and assets grows as most of banking operations are nowadays virtual and more operations are digitalizing.

Because of rapid digitalization in the banking industry, the current cyber threats will evolve in the future as technology develops and becomes more widespread. A growing network of IoT devices, technological solutions, and systems offer a broad playground for criminal minds to implement malicious behavior. The insider threat should not be underestimated, as just one breach can cause major losses for an institution.

As stated before, cyber threats often originate from humans and thus cannot be neither perfectly predicted nor eliminated. The advancement of technology is strongly connected to the development of cyber threats, but the development of technological solutions used in the banking industry cannot be foretold in the long term. This makes it difficult to determine the evolvement of the cyber threat landscape in the banking sector. However, inspecting new technologies and their possible vulnerabilities that might cause cyber threats can be significant in determining the threat landscape. Realized cyber threats, such as breaches, need to be carefully analyzed to find the vulnerabilities in the system and possible new methods used to perform a cyber-attack. Although new technologies such as blockchain can enhance security, there will still be cyber threats as no technology is perfect and new technologies also include security concerns.

Banks operate on the same principle and provide the same basic services globally. Banking services might still vary in different countries because the development and implementation of technological solutions may not proceed simultaneously depending on the geographical area. However, cybercrime is not geographically limited but extends globally because of the borderless nature of cyberspace. Therefore, the findings of this research can be utilized regardless of a bank's geographical location yet considering the state of technological advancement in a certain bank. This thesis examined mainly the threats caused by human factors, such as cybercrime and insider threats. However, not all forms and techniques of cybercrime could be examined due to broadness of the subject. In addition, exceptional circumstances, such as natural disasters, that may cause cyber threats were not in the scope of this research. When considering the findings of this research in practice, also other aspects of threat factors should be considered.

Future work in the field should address the development and improvement of the applications that utilize emerging technologies to make them more secure. Regulation and standards are needed to harmonize the operations of FinTech companies. This also calls for research, as the operations are global and regulations within different regions need to be considered. The fact that FinTech companies are usually not subject to financial sector's regulation raises a security threat. It is important that as the digitalization of the banking industry progresses, customer data and assets remain secured.

REFERENCES

Abeeku, S. E., Agoyi, M. & Agozie, D. (2021). Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. *PeerJ Computer Science, 7*, e658.

Ali, L. (2019). Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC). *The Journal of Developing Areas, 53*(1), 267-279.

Baba, C., Batog, C., Flores, E., Gracia, B., Karpowicz, I., Kopyrski, P., Roaf, J., Shabunina, A., van Elkan, R. & Xu, X. C. (2020). *Fintech in Europe: Promises and Threats.* IMF Working Paper.

Barone, A. (2021, March 21). *What Is a Bank?* Assessed February 2, 2022 https://www.investopedia.com/terms/b/bank.asp

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M. & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access, 9*, 61048-61073.

Blauner, C. (2013). Cybersecurity and the Banking Sector. *Hampton Roads International Security Quarterly*, 54-60.

Broby, D. (2021). Financial technology and the future of banking. *Financial Innovation, 7*(1), 1-19.

Canadian Centre for Cyber Security. (2021, June 29th). *Cyber threat and cyber threat actors.* Assessed November 14, 2021 https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

Carin, B. (2017). G20 safeguards digital economy vulnerabilities with a financial sector focus. *Economics: The OpenAccess, Open-Assessment E-Journal, 11*(19), 1-11.

Caporale, G. M., Kang, W. Y., Spagnolo, F. & Spagnolo, N. (2020). Non-linearities, cyber attacks and cryptocurrencies. *Finance Research Letters, 32*, 1-7.

Creado, Y. & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime, 27*(3), 771-780.

Das, S. R. (2019). The future of fintech. *Financial Management, 48*(4), 981-1007.

Dong, Z., Luo, F. & Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy, 6*(5), 958-967.

ECB. (2021a, August 18). *IT and cyber risk: a constant challenge.* Assessed January 18, 2022 https://www.bankingsupervision.europa.eu/press/publications/newsletter/2021/html/ssm.nl210818_3.en.html

ECB. (2021b, September 30). *Cyber risks and the integrity of digital finance.* Assessed January 18, 2022 https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210930~e58b5eed9b.en.html

Europol. (2021a, December 7). *European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime.* Publications Office of the European Union, Luxembourg. Assessed March 25, 2022 https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

Europol. (2021b, December 7*). Internet Organised Crime Threat Assessment (IOCTA) 2021.* Publications Office of the European Union, Luxembourg. Assessed March 25, 2022 https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Farshadkhah, S., Van Slyke, C. & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security*, 100.

Gan, Q., Lau, R. Y. K. & Hong, J. (2021). A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach. *Technology Analysis & Strategic Management*, 1-17.

Gang, K., Özlem, O. A., Hasan, D. & Serhat, Y. (2021). Fintech investments in european banks: A hybrid IT2 fuzzy multidimensional decision-making approach. *Financial Innovation, 7*(1), 39-39.

Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K. & Aparicio-Navarro, F. J. (2018a). Detection of advanced persistent threat using machine-learning correlation analysis. *Future Generation Computer Systems, 89*, 349-359.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. & Baker, T. (2018b). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986-5002.

Giacchero, A. & Moretti, J. (2021). A possible holistic framework to manage ICT third-party risk in the age of cyber risk. *Risk Management Magazine, 16*(1), 30-42.

Guo, Y. & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation, 2*(24).

Haw, I. M., Ho, S. S.M, Hu, B. & Wu, D.. (2010). Concentrated control, institutions, and banking sector: An international study. *Journal of Banking & Finance, 34*(3), 485-497.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. & Ochoa, M. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys, 52*(2), 1–40.

Joint Task Force Transformation Initiative. (2012). *Guide for Conducting Risk Assessments (Special Publication 800-30)*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Kellezi, D., Boegelund, C. & Meng, W. (2021). Securing Open Banking with Model-View-Controller Architecture and OWASP. *Wireless communications and mobile computing*, 1-13.

Khan, A., Mubarik, M. S. & Naghavi, N. (2021). What matters for financial inclusions? Evidence from emerging economy. *International Journal of Finance and Economics*, 1-18.

Klimburg-Witjes, N. & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses. *Science, Technology, & Human Values, 46*(6), 1316-1339.

Lallie, H. S., Shepherd, L. A., Nurse, J. R.C., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 1-20.

Meng, S., He, X. & Tian, X. (2021). Research on Fintech development issues based on embedded cloud computing and big data analysis. *Microprocessors and microsystems, 83*, 103977.

Mitnick K.D. & Simon W.L. (2002). *The art of deception: controlling the human element of security.* Wiley, Indianapolis.

Nicholls, J., Kuppa, A. & Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access, 9*, 163965-163986.

Noor, U., Anwar, Z., Amjad, T. & Choo, K.-K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems, 96*, 227-242.

Osmani, M., El-Haddadeh, R., Hindi, N., Janssen, M. & Weerakkody, V. (2021). Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. *Journal of Enterprise Information Management, 34*(3), 884-899.

Padmaja, K. & Seshadri, R. (2019). Analytics on real time security attacks in healthcare, retail and banking applications in the cloud. *Evolutionary Intelligence, 14*(2), 595-605.

Palmié, M., Wincent, J., Parida, V. & Caglar, U. (2020). The evolution of the financial technology ecosystem: An introduction and agenda for future research on disruptive innovations in ecosystems. *Technological forecasting & social change, 151*, 119779.

Sailio, M., Latvala, O.-M. & Szanto, A. (2020). Cyber threat actors for the factory of the future. *Applied Sciences, 10*(12), 4334.

Smith, T. & Stamatakis, N. (2020). Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns. *International Journal of Cyber Criminology, 14*(2), 433-459.

Templier, M. & Paré, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of the Association for Information Systems, 37*, 112-137.

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

Wang, J., Gupta, M. & Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly, 39*(1), 91-112.

Warkentin, M. & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52*, 102090.

Weissman, M. L. (2017). Employee's Negligence Contributing to a Fraudulent Transfer Did Not Nullify Bank's Insurance Coverage. *The RMA journal, 99*(6), 71.

Willison, R. & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly, 37*(1), 1-20.

Ye, C., Cao, W. & Chen, S. (2020). Security challenges of blockchain in Internet of things: Systematic literature review. *Transactions on Emerging Telecommunications Technologies, 32*(8), e4177.