Nathan Pruzina

Due: 09/28/2021

George Mason University

Randolph Terlecki, Mahesh Kumar Nainapally, and Vaishnavi Kammalampundi

IT 104- Section 103 Lab 206

Cybercrime in the Banking Industry: Threats and Protective Measures

Introduction

Banks serve as some of the most regulated and secure institutions in the world. However, this fact does not prevent criminals from exploiting their vulnerabilities. Cyber-attacks, including malware, phishing, and distributed-denial-of-service (DDoS), are the three main methods hackers use to infiltrate financial institutions (Franklin 2). Every established business, not just banks, is susceptible to cyber-attacks today; the digital sovereignty of every person, in fact, is at risk at a moment's notice. Cyber security goes hand-in-hand with cybercrime, and must be dealt with a low tolerance of failure. Consequently, the responsibility of protecting the integrity of financial institutions and their clientele rests heavily on security managers. The topic of cybercrime in relation to banking has grown as a relevant topic over the years. Mark Camillo, head of cyber, EMEA at AIG states, "…even though banks are some of the most mature entities when it comes to incident preparedness, and they have spent quite a bit on this over the years, they are still susceptible to breaches." A source from 2018 claims that cybercrime and cyber-related issues have cost the financial sector an astounding 18 billion dollars a year (Labbe 1). Contemporaneous suggestions even consider these digital invasions a domain of cyber warfare, which can directly impose great consequences larger than that of money and banking (Kari 1). However, this research paper will avoid discussing political and nationwide issues of cyber security. Rather, a more discussion on the current uses of cyber security in the banking industry will be discussed. Common security aspects and legislation will also be touched upon, along with ethical and social implications. Finally, the future uses of these protective tactics will be considered as the presence of cybercrime becomes more diverse.

Current Use and Threats

The risks associated with cybercrime grow day by day (Ali 1). Cyber criminals transcend the boundaries of traditional crime with their use of computers, mobiles, and other network devices key to committing such attacks. The three most common cyber-attacks include malware, phishing, and DDoS.

Malware itself can constitute a variety of terms, but it is typically defined as software created to damage, disrupt or rupture access to a computer system or network (Franklin 2). The most common form of this malicious software includes viruses and ransomware, which are specifically designed to penetrate a network through a weakness or flaw. One of the most prominent malware attacks on the banking industry followed the development of a new virus called Trojan-Banker.Win32/64.Neverquest (Neverquest for short) (Caulderwood 1). Trojan viruses are a type of malware that appears benign to unsuspecting users. When downloaded onto a computer, either remotely or through a link, the virus modifies the contents of your web browser (e.g., Chrome, Firefox, Edge), making it seem like a user must re-input their login information for recent websites. Instead, these usernames and passwords are sent to hackers, who then use virtual network computing to gain access to your account remotely. “This gives malicious users the chance to not only transfer cash funds to their own accounts, but also to play the stock market using the accounts and money of Neverquest victims,” wrote Sergey Golovanov, researcher at Kapersky Lab, a Russian computer security company (2).

Phishing is another method used to infiltrate financial institutions, and can be defined as sending fraudulent messages posing as a reputable source in order to convince recipients to disclose sensitive information, including bank account numbers and routing numbers (Padmaavaathy 4). This cyber attack typically takes form as an email, shepherding unknowing

victims to a website where they are asked to update personal information, whether its banking information, a social security number, or password. These details are then used by the perpetrator to commit identity theft. Emails of this nature are usually sent to large groups of people to increase a hacker's odds of success.

The last commonly used method includes Distributed Denial of Service attacks, or DDoS for short. DDoS attacks are a complex variation of regular denial of service attacks, which consists of flooding a network (usually a router or communication server) with spam or other useless traffic (Padmaavaathy 3). This effectively denies a user from utilizing a service that they are entitled to access or administer. DDoS attacks complicate this type of attack by sending these stale requests from multiple remote locations, thus making it almost impossible to track the source of the attack. What makes DDoS attacks unique is that they do not attempt to breach the electronic security perimeter of a business or individual. Rather, it denies legitimate users entrance to a website or server. These types of attacks can come in varying lengths and can affect a server for several weeks. Experts of the field suggest that DDoS attacks can also be used a distraction for other malicious activities when affecting online traffic.

To combat this sort of crime, banks must invest in an adaptable set of systems, and people to run them. Joe Nocera, cybersecurity and privacy financial services industry leader states, "The coordination and information sharing they we have seen around threat intelligence, sector wide incident readiness and systemic resiliency are all leading practices that other industries could model" (Labbe 3). In other words, coordination among a broad scope of financial institutions is the first step in stopping such crimes.

Security Aspects and Protective Measures

Efficient cybersecurity tactics are needed now more than ever to counter the invasive-nature of these attacks. One way to defend against cyber threats includes collaboration among central banks, commercial banks, and government authorities (Franklin 2). In this way, it can be seen that cyberattacks against banks affect more than just financial institutions themselves. "Cooperation is essential to strengthening resilience toward cyberattacks, especially since cyber-threats are global", said a member of Sweden's Riksbank (3). According to the same source, Riksbank is part of the European System of Central Banks, a collaborative organization intended for European banking. National institutions have also been created to encourage collaboration. Hans Van Loon of the Dutch Banking Association states, "In the Netherlands, we have the TNO (National Research Institute) that investigates the next generation of solutions to this issue, and ensures that we have the appropriate cybersecurity technology available. It has also pushed for innovation to be available to the market earlier on." Clearly, banks working together to prevent cybercrime is paramount for the protection of its assets and reputation.

Despite the potential benefits of transnational cooperation, issues still remain. Andrew Beckett, managing director of Kroll's Cyber Security, states, "One thing that is holding back big business is the lack of coordination globally and ever-increasing standards. It's also a delicate balancing act: businesses have to weigh up the cost of complying, the potential fines and the loss of a business license –on a global scale - with the level of risk that they face" (Labbe 2). For example, the European Union, Singapore, and United States all have different definitions of cyber preparedness and countermeasure effectiveness. International standards have been enacted; however, individual organizations and banks must determine their own level of risk and how to

address such discrepancies. Often, they must abide by several sets of laws from several different countries, thus blurring the lines of international banking.

In spite of the lack of a definitive framework for financial institutions, banks have found ways to prepare for cyber attacks without the risk of breaking international standards. “Cyber war exercises” such as Quantum Dawn and Sheltered Harbour served as simulations for more than 80 international financial institutions in 2016 (Labbe 3). Backed by government funding, this activity served as an unprecedented security exercise to help improve the industry’s resiliency and readiness against cyber-attacks. More specifically, the Sheltered Harbour Initiative acts as a safety net for banks by protecting and redeploying customer data if an attack were to happen.

Ethical and Social Implications

A breach of security in a financial institution could mean billions of dollars lost among those utilizing banks for their savings. Therefore, banks not only have to protect themselves from these attacks, but their entire client base as well. This fact complicates the implementation of cybersecurity measures because of its underlying stress on ethical and social implications. Consider the following statement by JP Morgan in 2016, “JPMorgan Chase and other companies . . . have reported significant breaches in the security of their websites, networks or other systems, some of which have involved sophisticated and targeted attacks intended to obtain unauthorized access to confidential information, destroy data, disrupt or degrade service, sabotage systems or cause other damage, including through…cyber-attacks… (Skinner 264).

Statements such as the latter urge the public toward a negative perception of the financial services sector, especially when dealing with ethical and social issues (Federwisch 1). However, since the financial industry includes banks, securities firms, pension funds, mortgage lenders,

and more, the public tend to group these headlines into the ethical mistakes of the banking sector. Ethics leader James A. Mitchell of the University of St. Thomas states, “This business that we’re talking about is really big. It is, to be precise, $50 trillion in assets. It’s growing 8 percent a year, which is more than twice as fast as the gross domestic product. It’s also highly profitable. The financial services sector of the S&P 500 represents 20 percent of this index’s market capitalization. These companies are making a lot of money serving you.” Though these companies appear to be losing large quantities of money from cybercrime, sources say that these losses only comprise a small percent of the absolute gains. It is also important to mention that the banking industry is extremely regulated, thus forcing companies, such as JP Morgan, to report on cyberattacks. Legislators force these companies to remain transparent to protect the general public from social and ethical discrepancies.

Future Use

The behavior and methods used in cyberattacks are constantly changing. Defending an institution against possible attacks involves permanent monitoring and protection against the most sophisticated attacks. Institutions such as JP Morgan, Bank of America, and Citigroup have all reported explicit intrusions of cyber risk in past years (Skinner 266). Who’s to say these breaches aren’t realized on a daily basis? As previously mentioned, it is key that the banking industry as a whole works to collaborate to maximize protective measures. In the future, legislators must come together to re-establish laws that cultivate international collaboration against cybercrime. As the world becomes more technologically based, online criminals obtain more outlets for their transgressions. The evolution of banking services on the digital realm has inevitably proved this point, distributing mobile banking into the hands of every individual with a mobile device. Protecting against these attacks will only become a bigger threat, therefore

financial institutions must work together to protect their assets, as well as the wealth of their clientele.

References

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. http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/cyber-crimes-constant-threat-business-sectors/docview/2094395116/se-2?accountid=14541

This research paper deals with the issues of cybercrimes and discusses how cybercrime activities effects the growth of the business sectors especially in the region of Gulf Countries Council (GCC). The data of the research is collected through survey questionnaire from employees of banking sectors and from general public and discussion is formed on how security measures could be further strengthened to improve the level of online banking security as well as the business growth in GCC. The importance of additional security devices to enhance the levels of security of online banking is also discussed. The research findings shows that cybercrime is one of the important issues that should be properly tackled by the banking and financial industry in GCC as the effects of cybercrimes are more than the financial integrity of financial institutions and other organizations.

Caulderwood, K. (2021, January 7). *New computer virus targets banking sites to steal your info, experts warn*. International Business Times. Retrieved September 20, 2021, from https://www.ibtimes.com/new-computer-virus-targets-banking-sites-steal-your-info-experts-warn-

1488356#:~:text=A%20Trojan%20is%20a%20kind%20of%20computer%20virus,websites%20opened%20in%20Internet%20Explorer%20or%20Mozilla%20Firefox.

This newspaper article highlights the development of a new virus that can steal your banking information. The new virus, called Trojan-Banker, is particularly unique because of its apparently benign access when downloaded. After download, it infects a website or computer and performs its task. In this case, Trojan-Banker steals your banking information. It does this by allowing hackers to gain remote access to your computer.

Federwisch, A. (2015). *Ethical issues in the financial services industry*. Markkula Center for Applied Ethics. Retrieved September 25, 2021, from https://www.scu.edu/ethics/focus-areas/business-ethics/resources/ethical-issues-in-the-financial-services-industry/.

Ethical issues in the financial services industry affect everyone, because even if you don't work in the field, you're a consumer of the services. This misperception persists for several reasons, Mitchell said. First of all, the industry itself is quite large. The industry is also highly regulated, so it's likely that a higher percentage of these bad transactions are identified and reported, perhaps more so than in other less regulated industries. Ethical lapses do occur, and Duska discussed five reasons why these misdeeds may happen. He holds the Charles Lamont Post Chair of Ethics and the Professions at The American College. The Post Chair supports research and studies of the social responsibilities and ethical challenges facing the financial services industry.

Franklin, J. (2019). Central banks struggle with cybersecurity too. *International Financial Law Review,* http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/central-banks-struggle-with-cybersecurity-too/docview/2304752336/se-2?accountid=14541

The gatekeepers of the global economy are coming up against many of, if not more than, the challenges that cybersecurity poses to the private sector Since the establishment of the Bank of England in 1694, the concept of central banks has evolved significantly. KEY TAKEAWAYS A recent attack on the European Central Bank has seen central bank cyber security again come to fruition; The Bank of America and the Bank of Spain have also endured attacks in recent years; Central banks are have both the risks of regular financial institutions and more, when it comes to ensuring they're protected against possible attacks. ...]it's possible that the contact data – but not the passwords – of 481 subscribers to the BIRD newsletter may have been captured.

Kari, M. (2019). *Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats*. Academic Conferences International Limited.

The Information Security Doctrine of the Russian Federation (RF) defines the threat to information security as a complex of actions and factors that represent a danger to Russia in the information space. These threats can be information-psychological (i.e., when the adversary tries to influence a person's mind) or information-technical (i.e., when the object of influence is the information infrastructure). The information infrastructure of the RF is a combination of information systems, websites, and communication networks located in the territory of the RF, or those used as part of international treaties signed by the RF.

Labbé, A. (2018). PRIMER: banks and cyber security (part 1). *International Financial Law Review,* http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/primer-banks-cyber-security-part-1/docview/2012825779/se-2?accountid=14541

According to Andrew Beckett, managing director and EMEA leader for Kroll's cyber security and investigations practice, banks need to understand the nuance of geographical requirements, which can sometimes make compliance very difficult. The focus has historically been on best practices. “Because of the lack of prescriptive frameworks - threats are so fast-evolving - banks tend to follow ISO standards ISO 27001 is the international standard for best practice information security management systems] to address cyber security,” said Camillo. What are Sheltered Harbour and Quantum Dawn? Because the digital landscape changes constantly – as do the threats banks face – there is no single fail proof way of staying safe.

Padmaavathy, P. A. (2019). CYBER CRIMES: A THREAT TO THE BANKING INDUSTRY. *International Journal of Management Research and Reviews, 9*(4), 1-9. .

Cybercrime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity. As cyber-attacks continue to plague businesses, it is banks who are under the greatest scrutiny from the increasing threat. Criminals can send phishing emails or set up fake websites that dupe consumers into giving away sensitive financial data. They can also leverage information from social media sites to socially engineer their way into accounts via customer service. Compared to today, the secure bank of the future will use more machine-learning technology and systems to proactively prevent potential breaches and data loss.

Skinner, C. P. (2019). Bank Disclosures of Cyber Exposure. *Iowa Law Review, 105*(1), 239-281. http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/bank-disclosures-cyber-exposure/docview/2346692746/se-2?accountid=14541

Financial institutions are increasingly subject to cyber incidents and attacks. Cyber intrusions threaten these institutions' balance-sheets and reputations, and can undermine their resilience. From a societal perspective, cyber risk is particularly concerning as it regards systemically important financial institutions, like the largest internationally active banks. This is because the stability of the financial system as a whole-and thus the real economy-depends on these banks' resilience to stressful events, including cyber attacks. To date, the SEC has taken the lead among the financial regulators in addressing cyber risk, chiefly through an emphasis on disclosure. This Article critically examines the existing design of that mandatory disclosure regime by reviewing the content of nearly 900 SEC filings made by the seven systemically important U.S. bank holding companies over a three-year period. That review suggests that the current trajectory of SEC rules and guidance is in some ways overbroad as applied to these institutions; but in other ways, the rules and guidance remain inadequate to address the various public and private interests at stake. The Article urges the SEC to design a more nuanced set of rules for cyber disclosure, which would be better tailored for systemically important banks.