Fall 2017

Analyzing Cyber Threats Affecting the Financial Industry

Anna Skelton
Embry-Riddle Aeronautical University

Analyzing Cyber Threats Affecting the Financial Industry

Directed Study Fall 2017

Anna Skelton

In collaboration with Jesse Laeuchli

Edited by David Ehrensperger

Table of Contents

Abstract

As critical infrastructure, financial institutions must execute the highest level of cybersecurity as the threat of a crippling cyberattack continues to develop. Malicious actors, including disenfranchised employees, state sponsored actors, and traditional hackers, all have motivations to target the financial industry, and do so frequently. However, the threat changes slightly between resource rich large institutions and their smaller, community bank counterparts. The complex and multifaceted threat must be fully understood in order to properly address and analyze solution options to preserve the security of these institutions and the economy that they contribute to.

Introduction

Financial institutions are a key foundational element, both to the United States and the world as a whole. As critical infrastructure and keepers of currency, shocks felt in the industry can reverberate, with extreme consequences, into every element of American life, as illustrated in the financial crisis of 2008. While banks, both monumentally large and humbly small, fulfill the expectations to keep the variable global economy relatively stable, the threat of cyberattacks on such institutions continue to emerge. Every year, malicious actors, a category that contains from state sponsored hackers to disenfranchised insiders, attack banks through technical means. Some attacks are financially motivated; some seek simply to disrupt and cause the chaos that happens when critical infrastructure is seriously threatened. Data breaches, a common form of attack, leave millions of customers' confidential information up for grabs. This conglomeration of destructive factors has lead the finance industry to be the highest spender on cybersecurity- even higher than the government. (Lagazio, Sherif, Cushman) Although available literature has analyzed the threat from many perspectives, two key areas require a more in-depth analysis; the unique situation faced by small and community banks, and the insider threat faced by companies of any size. By understanding and dissecting the threat faced by financial institutions, the increased awareness makes it easier to analyze solutions and look towards the future of the issue.

The threats faced by financial institutions vary widely in in source, modality of attack, and motivations of attackers. Attackers can be generally divided into three groups, with each group exhibiting a trend in their attack method and goals. The first group, resentful employees, often seek to disrupt business, potentially through a damaging data breach or through sharing company trade secrets. (Cummings, Lewellen, McIntire, Moore. Trzeciak) Their methodology

can be accidental, negligent, or malicious. (SentinelOne) Secondly, state actors often attack the accessibility of resources through Designated Denial of Service (DDOS) attacks. Although some of these attacks aim to extract capital, like North Korea, the objective is usually to disrupt or ruin the reputation of the bank. (Strategic Finance) The final group consists of individual hackers or hacker "collectives" that are difficult to pin down, using skill a complex arena of security concepts to extract money or data that can be anonymously sold on the dark web to the highest bidder. (Feeney)

Collectively, these attacks can be extremely difficult to prevent. The threat evolves at speeds that make building and maintaining defenses almost impossible. Though the government has implemented a series of policies to ensure financial institutions stay secure, the burden of the responsibility falls on the firms themselves- to buy, build, and defend a cyber-infrastructure of their own, including ensuring that any third party vendors are also secure lest they be an avenue into the institution for a malicious actor. (Mohammed) For small banks, this price tag can seem astronomical, surpassed only by the consequences of a cyberattack. (Abend)

Definitions

It is imperative, when discussing cybersecurity, to clarify terms. In this paper, "financial industries" will be defined as "a vast assortment of firms, agencies, and institutions with operations ranging from small community banks to massive, international corporations" (Mohammed). The term will be used interchangeably with "banks". Malicious actors are defined as "an entity that is partially or wholly responsible for a security incident that impacts- or has the potential to impact- an organization's security" (BeyondTrust.com). The term "malicious actors" is used to describe all types of actors as above, and used interchangeably with the term "threat

actors." Cybersecurity will be a combined term, as to illustrate the unique threat faced by institutions that is indivisible and unique. (CyberPedia)

Understanding the Threat

The Department of Homeland Security lists the financial sector as critical infrastructure in the United States that is vulnerable to a variety of threats- including, perhaps the most pressing, the threat of cyberattacks. (DHS) A large-scale cyberattack could bring nearly every element of American life to a grinding halt. Depending on the attack, citizens might be unable to utilize their banking cards to purchase goods or extract cash, have their bank accounts emptied without a trace, or experience the consequences of an economic meltdown. For these reasons, the banking industry has a solemn responsibility for keeping customers and assets secure. However, the types of attacks face by banks are varied, intricate, and complex.

Malicious actors have no shortage of avenues into banks. Phishing, the practice of targeting unsuspecting employees with emails that allow threat actors onto their device or the company's network, are extremely successful despite training programs because no amount of security software can completely mitigate human fallibility. This can also be true of websites embedded with malicious software that threat actors lure employees and bring down a system in a single click. State actors or malicious actors hoping to gain access to a firm's internal system frequently utilize phishing.

Once malicious actors have gained access into a system, two scenarios can play out. If the bank has security measures in place within the bank's online systems, the threat actor can be stopped or at least slowed down as the intruder is forced to develop another solution. Sometimes, these malicious actors are slowed down to the point where they can be detected by security

specialists monitoring the intranet. Alternatively, if a firm has not invested in these additional security measures, a malicious actor will have free reign to all resources, from employee and consumer data to trade secrets. (Mitnick) In the 2013 Carbanak attacks, for example, a method known as spear phishing was used to install bank employee's computers with malware that allowed threat actors to capture video footage of bank employees completing key daily activities, such as transferring funds and bypassing security measures. These attacks alone affected more than 100 banks and stole a range of $2.5 million to $10 million from each bank. (Johnson) For this reason, it is imperative that firms have online security measures in place for both internal and external threats.

Third party providers also supply an often-overlooked path into a company. Any firm that provides services to the bank, ranging from health care providers to cloud service providers, has their own cybersecurity measures. Malicious actors could potentially exploit a vulnerability in the third party's cybersecurity to trespass into the intended target. Larger financial institutions may have the resources to ensure their third party suppliers are secure, but few factor this key element into their cybersecurity program, and most small or community banks cannot afford it. (Feeney) Third party vendors are an increasingly large target for state sponsored actors looking for avenues into a firm's network. Malicious actors seeking a data breach can utilize the trusting connection between third parties and firms to expose sensitive data.

Finally, the growing use of internet and mobile banking provides an easy way for malicious actors to access resources and commit fraud. (Castelluccio) Banks frequently enact security measures that are rejected by consumers for complicating a process sold on based on its perceived convenience. (Fattahleh, Mercadi, Meharia, Panja, Robinson) However, by rejecting these measures, customers inadvertently put themselves at risk for fraud. A study by a collection

of students at the University of Michigan found that accessing a mobile banking account on a device is astonishingly simple, as many of the security features are disabled by the consumer. The authors of the study found that if a consumer has disabled the screen lock on the mobile device and opted for the auto-filling of the mobile banking username associated with their account, the malicious actor needs only to crack the password to gain complete and unfettered access into the account. (Fattahleh, Mercadi, Meharia, Panja, Robinson) Although many banking institutions insist on passwords that feature a variety of characters and must be changed regularly, customers frustrated with the task of frequently conjuring a new complicated password often opt for only slight iterations of their previous password. Malicious actors with a focus on password cracking find many of these passwords, the majority of which follow a basic pattern (numbers and characters at the end, alphanumeric substitutions) to be easily exploited. (Rankin) Once access into the account is gained, it is easy to begin the process of fraud.

These fraudulent attacks are an easy way for cybercriminals to profit. Media has portrayed this circumstance dramatically, insinuating that malicious actors can empty bank accounts with a single click and still manage to avoid prosecution or identification. (Close-Up Media) However, in order to keep their malicious intentions hidden and to remain covert, most of these attacks follow a pattern of taking negligible amounts of money- say, a few cents to a few dollars- out of an account. These infinitesimal extractions are extremely challenging for fraud investigators to identify and pursue, and are often lost in the noise of millions of daily transactions. (Bronk, Monk, Villasenor) However, taking small amounts of money from thousands or millions of accounts can easily add up to numbers in the millions. In fact, a book addressing the issue published in 2016 states that US$1 billion has been hacked from banks since 2013, demonstrating the severity of the issue at hand. (Taplin)

In a recent related case, malicious actors we now know to be associated with North Korea seized US$81 million from the Bangladesh Bank's account at the Federal Reserve Bank of New York. (Reuters) These funds are likely being used to fund the North Korean missile development program. This attack itself was relatively simple and intuitive, and the transfers were allowed even though none of the requests were formatted correctly in the first place. Though the majority of their intended financial gain was blocked (the original goal was $951 million), US$81 million is still a hefty sum for a situation that could have been avoided with more internal safeguards. (Bukth, Huda) Just like with successful terrorist attacks, it is almost guaranteed there will be copycat attacks in the future.

Despite the obvious threats, the financial industry as a whole is woefully underprepared for such attacks. Although a PricewaterhouseCooper study found that 75% of surveyed banks intended to increase funding for cybersecurity in the next twelve months, another longitudinal study found that 54% of their respondents say "financial loses aren't high enough from cyberattacks to warrant broad level attention". (Wee, Close Up Media) Considering the above information, this simply is not true. In fact, the same article, published by Finance Asia includes a quote from a key cybersecurity professional that "[The banks my firm has worked with] have all been compromised to some extent. Everyone we have investigated has had a breach. Every bank that we have done an assessment has been compromised by malware they didn't know was there". (Wee) Additionally, a study conducted by the Ponemon Institute found that "organizations that utilize security intelligence technologies reported having significantly lower costs than organizations that did not employ them". (Johnson) Clearly, a severe disconnect exists between the threats perceived by the banks and the actual threat that exists from malicious actors.

This disconnect was demonstrated in a study conducted by two students at Dakota State University that compared the self-disclosed cybersecurity risks of large U.S. banks to the actual threat as found by the Securities and Exchange Commission. Underreporting of risks is chronic although not always intentional; as banks strive to show customers that the money they entrust is safe. However, "these inaccuracies can result in an inflated stock price and a reduced understanding of the corporations true information security risks" which could have devastating consequences should a firm that has underreported become a target of a well-executed cyberattack. The study found that "in 2014, the study entities did not report 33% of the risks found within their business domains". Thirty-three percent is a significant number that could easily have severe consequences if not addressed. The study found that as banks mature cybersecurity programs and receive increased guidance on reporting, the number of risks decreases. (Bakker, Streff)

Bank Size versus Threat Faced

When approaching this extremely nuanced issue, one of the key factors to be analyzed is the impact that the size of a financial institution has on the types of attacks they face and their defenses against them. Although it may seem like an obvious solution for large banks with plentiful resources, employing this strategy exclusively is unlikely to provide a long-term solution to the complex issue at hand. Interestingly, many large institutions have been found that "overspending on defense measures and chronic underreporting has also had an important consequence at both overall sector and society levels, potentially driving the cost of cybercrime even further upward". (Lagazio, Sherif, Cushman). These large institutions may have the resources necessary to create a significant security platform, but they are misused, leading to, in some cases, a widening of the security gap. However, if an attack did occur, the bank could point

to the money spent on cybersecurity to relieve the blame and attempt to reassure customers. In fact, some banks have band-aid policies in which, instead of identifying the underlying issue, a vulnerability is simply patched or a new protocol written. This leads to a convoluted maze of overlapping patches and redundant protocols. (Mohammed)

For smaller banks, who have fewer financial resources to devote to cybersecurity, the threat only multiplies in size. According to one source, community banks compose over 96% of all U.S. Banks (Westchester County Business Journal). If this figure is to be believed, community banks are even more fundamental to protect in the eye of the cyber threat. A Chief Information Security Officer at a small bank on the East Coast put it bluntly, "smaller banks still have the same challenges as larger banks do, but not the same resources". (Westchester County Business Journal) To put the issue in perspective, a Symantec study reported that half of attacks aimed at financial institutions targeted those banks with less than 2,500 employees. However, smaller banks are more likely to be aware of the risk, as 85% reported being extremely concerned about the cyber threat. (Bank Director).

Of course, everyone has a different theory on what is the best course of action for smaller institutions to pursue. If smaller banks cannot find the space in the budget to create an entire department dedicated to cyber defense, it would be advisable to hire third party security providers to monitor their networks (not to be confused with third party providers of other services noted as a vulnerability above). (Abend) A benefit of utilizing third party security providers comes with the ability of these providers to process threat data, including data from intrusion detection systems and firewalls, which would simply be impossible for a small bank's security department to properly process. (BankNews) A key regulator at the Office of the Comptroller of the Currency recommends that community banks start by conducting a

comprehensive risk assessment that "1) identifies internal assets and processes, 2) describes external threats to themselves, third parties and the sector as a whole, and 3) outlines their vulnerabilities to these threats". (Abend) Public-private information sharing also provides an important opportunity for community banks to gain valuable threat intelligence at an inexpensive price. (Abend) Interestingly, community banks have already had success utilizing the close relationships with individual customers to inform them of the threats and disseminate information to improve the patron's security. In this way, small banks have a strength that impersonal big banks lack.

The Insider Threat

However, nothing renders banks immune to one of the most severe threats faced by the banking industry with regard to cybercrime: the insider threat. A study conducted by the Software Engineering Institute defines a malicious insider as "a current or former employee, contractors, or other business partner who has or had authorized access to an organization network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems". (Cappelli). The study, deemed one of the preeminent pieces of literature on the subject, discovered six critical findings; criminals used a prolonged amount of low level activity both accomplished more damage and remained undetected for longer; insiders means were not frequently technically advanced; managers committing fraud accomplished much more damage than their non-manager counterparts; incidents of collusion were infrequent; audits are the best way to identify malicious employees; and personally identifiable information is the most frequent target of these attacks. (Cummings, Lewellen, McIntire, Moore, Trzeciak). This information is vital if companies are to take action against this dangerous threat.

Another study found three identifiable distinctions in the types of attacks conducted by insiders; accidental, negligent, or malicious. According to Verizon's 2016 Data Breach Incident Report as quoted by SentinelOne, 30% of insider damage was simply accidental- employees simply are not educated enough on cyber activity to utilize industry best practices. The next category, negligent damage, occurs when "employees try to avoid the policies you've put in place to protect endpoints and valuable data". (Sentinel One) Employees, like consumers, can be immune to measures carefully put in place to protect information in the name of laziness. Finally, malicious insiders are most likely to cause the most damage. This category could include employees that feel they have been treated unfairly, have become disenfranchised with the company, or have recently been laid off. These employees can conduct a variety of destructive threats, including extracting sensitive company data to which they have access and selling it to the highest bidder, or committing fraud with their resources to pad their own pockets.

Considering Consequences

The consequences felt by financial institutions in the wake of cyberattacks are nearly as destructive as the events themselves. As critical infrastructure, banks are vulnerable to one type of attack that other institutions may not be- the threat of the domino or contagion effect. Partially witnessed in 2008, the domino effect occurs when "one prominent entity of interconnected company [being attacked…leads to] sound financial institutions become viewed as weak, and panicked customers withdraw funds from sound entities, causing sound businesses to fail". (Weiss) Put simply, if one bank experiences a significant attack, it is likely that customers of other banks could become worried about the security of their money and withdraw their funds, causing banks that would otherwise be healthy to collapse as they do not have the actual assets to repay their customers. This is an end game scenario, in which a successfully conducted attack on

one bank causes a collapse in the national economy and, quite possibly, the world economy as well.

A more common and noted threat faced by financial institutions of shapes and sizes is that of data breaches. Data breaches can contain information regarding a variety of elements, including company trade information or personal information. One source notes that "cyber criminals love to loot employee or customer personal information, such as Social Security numbers, dates of birth, mothers' maiden names, addresses, account numbers and passcodes". (Muig, Smith, and Stambaugh) This information can be sold to any number of customers to use it for further nefarious purposes. A perfect and terrifying example of large-scale data breach was the infamous Equifax data breach of September 2017. Ultimately, the information of 145.5 million Americans, nearly half the population was released, causing a loss of confidentiality that is devastating and irreversible. (Moore) The company itself is likely to experience "stock market volatility and significantly reduced normal stock returns" after such a breach (Corbet, Gurdgiev) The damage does not stop after the information is released- secondary consequences, in which the released data is manipulated to cause further damage, are likely after a breach such as the Equifax cataclysm. Already, experts are predicting an increase in healthcare fraud and entitlement fraud as the consequences from this one cyberattack radiate into other industries. (Moore) It is easy to say that a solution could be found if customers had more control of how their data is used and distributed, but a lack of regulations about the following and the widespread willingness of customers to give their personal information to institutions they trust prove this is an over simplified solution. In reality, the threat to information is almost impossible to mitigate except by increasing security measures.

Exploring Solutions

Obviously, such a wide-ranging problem has a plethora of solutions to choose from, ranging from technical endpoint structures to increased government regulations. Some argue that, with the threat continuing to spiral, increasing the complexity and range of encryption is the only way to protect data from being stolen. (Castelluccio) However, taken individually, this solution is unlikely to stop malicious actors who enjoy the challenge of cracking measures like encryption. Regulatory issues are often a point of contention, as they can be perceived differently by different groups involved. However, overall government regulations are a great way to ensure a minimum bottom line of security for financial institutions. (Mohammed) However, in order to be effective, these regulations will need to be clearly written and enforced, challenges that have plagued the American government since its conception.

Information sharing is another arena that may show an opportunity for improvement. By creating voluntary public-private information sharing portals like those that already exist for physical threats, threat intelligence becomes a much more advantageous tool for protecting financial institutions. However, in order for such portals to be successful, companies would have to acknowledge the benefits enough to share their information.

Concerning the end-user space, experts have been floating the idea of multi-factor authentication (MFA) or nontraditional authentication efforts. In the words of one expert leading the charge, “In a world where bad actors already know most everybody’s name, Social Security number and address, it is grossly imprudent to continue to use a system where authentication is based entirely on information that we all know has been compromised”. (Moore) However, developing a new, secure system for authentication would take extreme amounts of time and resources, and may not even be accepted by the people it is intended to protect.

A problem faced by many companies that contributes to shaky cybersecurity is the lack of maintenance applied to keeping expensive cyber security platforms active and clutter-free- they require constant upkeep to remain active. Many times, companies will purchase these platforms assuming they are a one-step solution, but in reality these are only tools that require constant attention to remain productive at their full potential. One expert puts it simply, “cyber security isn’t a ‘set it and forget it’ situation”. (Morris)

Conclusion

Ultimately, the responsibility for cybersecurity of financial institutions lies with everyone it comprises of, from security engineers to C-suite officials to tellers to costumers. In order to thwart the monumental threat of malicious actors targeting banks, small and large banks must be acutely aware of the specific risks they face and prepared to face such risks appropriately. These malicious actors are not uniform. They include insiders, state sponsored actors, and cybercriminals looking to commit fraud. The types of attacks committed are as varied as the attackers, and no one solution will be sufficient to mitigate the problem. As banks are critical infrastructure whose collapse or damage could have significant consequences for the United States and world economy, innovative strategies must be paired with diligence to create an truly secure industry.

Resources

Abend, V. (2013). Greater Awareness; A Regulator's Perspective on Staying Secure Against Rising Cyber Attacks. ICBA Independent Banker, 46-47. Retrieved November 15, 2017.

Bakker, T. G., & Streff, K. (2016). Accuracy of Self Disclosed Cybersecurity Risks of Large U.S. Bank. Journal of Applied Business and Economics, 13(3), 39-51. Retrieved November 22, 2017.

Biswajit, P., Fattaleh, D., Mercado, M., Robinson, A., & Meharia, P. (2013). Cybersecurity in Banking and Financial Sector: Security Analysis of a Mobile Banking Application. 397-402. Retrieved November 13, 2017.

Bronk, C., Monk, C., & Villasenor, J. (2012). The Dark Side of Cyber Finance. Survival, 54(2), 129-142. doi:10.1080/00396338.2012.672794

Bukth, T., & Huda, S. (2017). The Soft Threat: The Story of the Bangladesh Bank Reserve Heist . Business Cases. Retrieved November 21, 2017.

Castelluccio, M. (2015). Emerging Cyber Threats. Strategic Finance: Technology Workbook, 55-56. Retrieved November 11, 2017.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector. Retrieved November 12, 2017

FBI prepares charges against North Korea over Bangladesh heist | News | DW | 23.03.2017. (2017, March 23). Retrieved November 15, 2017, from http://www.dw.com/en/fbi-prepares-charges-against-north-korea-over-bangladesh-heist/a-38081602

Feeney, S. (2017). Cybersecurity Without Breaking the Bank. Bank News, 12-14. Retrieved November 15, 2017.

Gurdgiev , C., & Corbet, S. (n.d.). Financial Digital Disrupters and Cyber-Security Risks: Paired and Systemic. Retrieved November 13, 2017.

Insider Threats in Cyber Security-More than Just Human Error. (2016). CSO. November 13, 2017.

Johnson, A. L. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. North Carolina Banking Institute, 20(1), 277-310. Retrieved November 13, 2017.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector. Journal of Computers and Security. Retrieved November 30, 2017.

Longitude Research Survey: Banks Lack Ammo to Battle Cyberthreats. (2013). Trade Journal . Retrieved November 14, 2017.

Mitnick, K. (2005). The Art of Intrusion.

Mohammed, D. (2015). Cybersecurity Compliance in the Financial Sector. Journal of Internet Banking and Commerce, 20(1). Retrieved November 11, 2017.

Moore, T. (2017). On the Harms Arising from the Equifax Data Breach of 2017. Critical Infrastructure Protection . Retrieved November 11, 2017.

Morris, M. (2014). Keeping Modern Bank Robbers Out of Your Business Accounts . Strategic Finance, 16-17. Retrieved November 11, 2017.

Rankin, K. (Writer). (2017, September 29). SEX, SECRET AND GOD: A BRIEF HISTORY OF BAD PASSWORDS. Live performance in Conference Center, Phoenix.

Rohrer, K. K., & Hom, N. S. (2017). Who's Responsible for Cybersecurity. Strategic Finance: Technology Workbook, 62-63. Retrieved November 12, 2017

Taplin, R. (n.d.). Managing Cyber Risk in the Financial Sector: Lessons from Asia, Europe, and the U.S.A.

Wee, D. (2015). Bank Hacks. FinanceAsia, 18-22. Retrieved November 17, 2013.

Weiss, N. E. (2011). Banking and Financial Infrastructure Continuity: Pandemic Flue, Terrorism, and Other Challenges. Journal of Current Issues in Finance, Banking, and Economics, 4(1). Retrieved November 11, 2017.

WHAT IS CYBERSECURITY? (November 16). Retrieved December 14, 2017, from https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security