Issues in Information Systems
Volume 22, Issue 1, pp. 63-74, 2021

https://doi.org/10.48009/1_iis_2021_63-74

How financial institutions address cybersecurity threats: A critical analysis

Amy Kay, *University of North Alabama, akay@una.edu*
Christian Hutcherson, *University of North Alabama, chutcherson@una.edu*
Calen Keene, *University of North Alabama, ckeene@una.edu*
Xihui Zhang, *University of North Alabama, xzhang6@una.edu*
Mark G. Terwilliger, *University of North Alabama, mterwilliger@una.edu*

Abstract

The financial industry has been a frequent and heavy target of cyberattacks. This trend is likely to continue as the cybersecurity threat remains high in the financial sector. Through a critical analysis of current risks, potential business strategies, and software and hardware strategies, a set of best practices is presented that will help prevent and mitigate cyberattacks for financial institutions. These guidelines should be used as a practical application for financial organizations and can also serve as a basis for future research.

Keywords: Cyberattack, Cybersecurity, Network Security, Security Breach, Financial Institution

Introduction

Threats to network security are ever-present. Reports of security breaches have become more common despite globally increased security measures. It is estimated that in 2015, more than 300 million customers' personal data had been stolen in the 15 largest documented attacks worldwide (Tauwhare, 2016). According to Newman (2018), the worst cybersecurity breaches of 2018 included: (1) more than 300 universities worldwide (including 144 U.S. universities) were attacked, and about 31 terabytes of data were stolen, which was estimated by the Department of Justice (DOJ) to be worth three billion dollars in intellectual property; (2) Exactis, a marketing and data aggregation firm, left about 340 million records exposed on a publicly accessible server; and (3) hackers breached Under Armour's MyFitnessPal app, compromising usernames, email addresses, and passwords from the app's roughly 150 million users. Network security has far-reaching implications for firms, individuals, government agencies, and the private sector. One sector that has been hard hit by security breaches is the financial sector.

Data security within the financial sector is especially relevant to all individuals because most people have business dealings with financial institutions, and many of these institutions hold personal data about individuals. Because a cyberattack on a financial institution can do irreparable damage, it is imperative that financial institutions take measures to prevent successful cyberattacks. In the case of a cyberattack, a comprehensive identification and mitigation plan should be in place and ready to deploy. Too often, corporations do not know the scope of the security breach until months after the attack. This increases the vulnerability of individuals who have been affected, and it certainly raises a question of confidence in the institution. In a 2015 survey, 82% of senior business leaders stated that their cybersecurity policy is not

discussed regularly at board meetings; specifically, only 26% of companies discussed their cybersecurity policy regularly, while 52% discussed it rarely (Camillo, 2017).

There are several different aspects of cybersecurity that need to be examined in order to comprehend the scope of the issue, as well as develop a plan to thwart and respond to these attacks. First, it is important to identify the cybersecurity threats faced by financial institutions. Second, it is important to understand what financial institutions are doing currently to prevent these attacks. Finally, it is important to review network security technology that can thwart cyberattacks and network infiltration. Based on all the different sources of information, a set of best practices can be presented to help financial institutions proactively prevent these attacks and decrease security vulnerabilities.

A 2017 report showed an increasing trend in cybercrime and resulting losses globally. Using data from 20 countries with a total population of 3.2 billion, 978 million people were affected and 44% of consumers were somehow impacted by cybercrime in that year. Also, 53% of consumers either experienced cybercrime or knew someone who had. Cybercrime victims lost $172 billion globally, which is $142 per victim, on average. These losses were not just financial. The average cybercrime victim had to spend an average of 23.6 hours dealing with the aftermath of the incident. The most common cybercrimes listed were hacking a device (53%), debit/credit card fraud (38%), compromised account passwords (34%), hacking email or social media accounts (34%), fraudulent online purchases (33%), and phishing scams (32%) (Farahbod et al., 2020).

Cybersecurity in the financial sector is a threat that affects everyone. It is vital to protect the sensitive information of consumers and their financial assets. In 2013, the European Commission set out a European Union (EU) Cybersecurity Strategy. The strategy (Tauwhare, 2016) aims to: (1) promote cyber resilience, (2) reduce cybercrime, (3) develop cyber-defense policies and capabilities, and (4) establish a coherent cyber policy for the European Union. With constantly changing and emerging threats, institutions must be proactive in terms of end-user education and stay ahead of the curve through deploying the most advanced technology. A lack of action or a lack of sufficient safeguards puts millions of people at risk. Therefore, it is essential to explore existing and potential threats, vital technologies that can thwart the danger, and best practices that will promote a safer technology environment.

Current and future network system threats

As technology becomes increasingly powerful and ubiquitous, network threats arise and adapt (Neville-Neil, 2017). There are multiple network threats currently faced by financial institutions on a daily basis. The significant increase in web-based services from financial institutions has unfortunately led to a higher vulnerability for the institutions and their clients. As the use and development of technologies such as online and mobile banking, email, text messaging, and virtual financing increase, network system threats continue to adapt, and new threats develop.

There is an abundance of system threats faced by financial institutions in the U.S. and worldwide. Some of the most prominent include, but are not limited to, identity theft, malware, ransomware, phishing, vishing, employee exfiltration, online banking fraud, and mobile banking fraud. These threats are commonly employed, both independently and in tandem. Not only do these methods put finances of individuals and businesses at risk, but they also cause significant risk for the financial institutions themselves. Each of these threats is unique and tends to have differing degrees of risk. Nonetheless, they are all risk factors that must be addressed by the network security teams.

Phishing is one of the most used methods by fraudsters to gain sensitive or confidential information in the financial industry. Phishing is often used as a gateway for other infiltration such as malware, ransomware, and vishing. The fraudster may send a seemingly legitimate email to an employee or customer. The email often mentions something urgent that incites panic, which may result in a hasty response by the recipient. A phishing email may ask an employee to give their system login credentials for a particular test or for a false human resource purpose. For an individual, the phishing email may ask the customer to either call a number to speak with a representative (who is also a fraudster and will pose as a representative of the company) or login with online banking credentials. Once the information is given, it opens a gateway for malware, ransomware, and other fraud. If this happens to a customer via online banking, the customer may have funds stolen from their bank account or credit product. If this happens to an employee, the risk is much more significant because the attacker may have access to the same sensitive information as the employee, which could lead to widespread risk for the company, as well as its employees and customers.

Malware is malicious software intended to disable computers and computer systems. Malware is especially prominent in financial institutions because it could grant hackers access to debit and credit card information, account numbers, social security numbers, phone numbers, addresses, etc. Malware is typically used to "lower the operating system integrity in order to steal user data and to modify data presented to the user" (Black et al., 2018, p. 760). One of the most significant threats malware poses is the fact that it can adapt and evolve. There are numerous different families of malware that are often updated and made more potent than prior versions. Because of this, financial institutions must complete extensive research and remain aware of all potential malware.

Ransomware, one of the newest iterations of malware, is becoming more common. Ransomware is essentially malware that blocks system processes until a certain sum of money, or ransom, is received. This payment is often requested in bitcoin or other virtual currency. Compared to most companies, financial institutions have larger sums of liquid assets available. This makes them a primary target for ransomware, and they must rapidly improve and maintain network security to prevent a breach that could be detrimental. In June 2017, TNT Express, a FedEx subsidiary, was infected with the NotPetya ransomware virus, and FedEx reported an estimated $300 million loss in earnings because of this (Shoorbajee, 2017). If a ransomware attack were to occur at a financial institution, the culprits of the attack may gain access to account numbers, social security numbers, employee identifications, etc. As a result, users of the system could be at risk for fraud and identity theft for a prolonged period of time. In addition to the loss experienced directly from the attack, institutions could face additional lawsuits and fines from individuals affected and federal organizations. To add perspective, Wells Fargo was fined one billion dollars after finding that "the company had failed to catch problems in its auto and mortgage businesses over several years."

Employees of financial institutions themselves often pose one of the most imminent threats to a network. The lack of encryption in emails and in other forms of data storage and communication offers an easy target for those seeking sensitive information. Employees handle unencrypted data daily, so there is a constant risk for any data being handled that is not encrypted. It is worth noting that "Encryption, in and of itself, is not a solution to securing a system" (Neville-Neil, 2017, p. 37). Encryption should be used in tandem with other security measures including proper employee network security training to mitigate risks.

In addition to the lack of encryption on many files containing sensitive customer and employee information, employees have been known to use personal emails, personal or public networks, dropboxes, storage devices, etc. This exposes personal information and marks a bullseye for hackers and data miners. Most often, an employee will not intentionally put the financial institution at risk, but poor risk

management leads to the mishandling of data and puts the network at risk. If the employee takes the work laptop to a coffee shop and connects to the coffee shop's free Wi-Fi, any information on the laptop could be exposed to the unsecured network. The employee may not be doing something malicious, but there is still significant exposure of confidential information that could easily be obtained. Carelessness and ignorance can be two of the most significant threats to network security.

With countless threats to network security revolving around the financial industry, there are often new methods and processes developed to combat fraudsters and hackers. Common practices have been developed to help companies prevent and mitigate some of these malicious attacks. While there are many systems available to protect financial networks, there is always room for improvement and a need to defend against ever-evolving future threats.

Current financial industry security processes

To assess financial institution cybersecurity risks, it is important to understand the current practices of these organizations. What follows is a critical analysis of current industry practices and government enforced practices. This is not intended to be a comprehensive list but is an overview of the generally accepted practices. Some of these practices include staff training, usage policies, risk assessments, access reviews, response plan development, security testing, and implementation of various software and hardware solutions. The first six areas will be reviewed here, and a more elaborate explanation will be later offered pertaining to the software and hardware practices.

In line with the employee threat presented in the previous section, staff training is an important line of defense for financial institutions. It is the responsibility of the financial institution to ensure that these employees know how to correctly use the information they access and be aware of any potential threats their access could pose to the organization. "Time has proven that people are, and will always be, the key to successful security" (Habersetzer, 2013, p. 66). One element is to train staff on how to identify threats such as phishing emails or malicious websites. As mentioned before, in the case of an internal employee, this can lead to attackers accessing the company's network or accessing sensitive company information. Since filtering out phishing emails is not always effective, it is important for staff to recognize these threats. To prevent these types of attacks, staff should be trained in identifying fraudulent attacks in order to keep the information on the company's network safe. Staff should also be trained on how to properly use the data they are presented and know what information is confidential. An employee can be just as harmful to a company as someone outside the organization.

To ensure that employees are acting in accordance with their jobs, companies should track employee activity within their systems to ensure that no malicious or unauthorized activity is occurring. Based on recent regulations for the state of New York, financial institutions in the state are now required to "monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information" (Simon & Murphy, 2017, p. 35). These types of user training practices should be reviewed and updated at least yearly to ensure that organizations are aware of the latest cyberattack attempts.

A usage policy statement is used to outline users' roles and responsibilities with regard to security. This is related to user training in that employees using the network need to understand what is considered acceptable use of the company network. However, it is up to the organization to set the guidelines for what is and is not accepted through a usage policy. This policy should include guidelines on security responsibilities, outline actions that could result in disciplinary measures, and explain how to avoid such irresponsible activity. This policy should also include partners of the organization as well. The suggested

sections within the policy include general use and ownership, security and proprietary information, unacceptable use, and policy compliance. These policies, when properly implemented, can be an important part of cyberattack prevention.

Risk assessments should also be conducted to identify risks pertaining to the network, network resources, and data. This task is intended to identify portions of the network and assign risks, or threat ratings, to each portion in order to prioritize security levels. Common rating levels are low, medium, and high. Low-risk systems are those that would not impact normal business operations or would not cause any legal or financial problems if compromised. Medium-risk systems would cause a moderate level problem for the business if they were compromised. High-risk systems are those that would pose a major business issue if they were impacted and could cause serious financial and legal problems. In the financial sector, examples include the main banking applications of TurnKey Lender and OLYMPIC Banking System. A risk assessment should be made for all systems involved in business operations, especially those that collect and store sensitive information. It is also necessary to review these assessments frequently as is mandated by the latest state regulations. The New York state regulations, for example, require risk assessments to be performed regularly and be kept up to date with the organization's changing infrastructure and business processes as well as the evolving threats (Simon & Murphy, 2017).

Access reviews are common in many industries and are especially needed in financial firms that deal with sensitive information. Access reviews help dictate access controls which limit the activity of legitimate users. These reviews consist of assessing who has access to a particular system and what information they are allowed to access. These systems can include network servers, data access, and applications and functions within a financial application. Not all employees will have the same access, nor should they. To protect systems best, the number of users that have access to these systems should be the minimum number needed for the organization to operate effectively and efficiently. Limiting the number of users accessing sensitive information will overall reduce the number of potentially malicious users and reduce the risk of compromise on the system (Habersetzer, 2013).

Many firms implement response plans, which are contingency plans for dealing with a cyberattack. In recent regulations dealing with the state of New York's financial industries, these plans should "promptly respond to, and recover from, any Cybersecurity Event that materially affects the availability, confidentiality, or integrity of the Covered Entity's Information Systems or the continuing functionality of any aspect of its business or operations" (Simon & Murphy, 2017, p. 35). These plans should have both a technical focus and a customer focus. The technical portion of a response plan should involve getting the system back operational after an attack. This also entails fixing the vulnerability in the system to avoid a repeat of the same attack. The new regulations in New York require a response plan that consists of clearly defined roles and responsibilities, external and internal communication processes, identification of the weakness, and documentation of the cyberattack (Simon & Murphy, 2017). A company's response should also have a customer focus in order to manage customer relations after an incident. Fathi (2016) suggests using social media to get out ahead of any potentially negative press after a cyberattack. It is important for a company to display urgency, empathy, and transparency so that the incident does not negatively impact the company's reputation or slow down recovery time (Fathi, 2016).

Security testing is another aspect of helping financial institutions prevent cyberattacks. There are several different strategies when testing networks, including vulnerability scanning, password cracking, and penetration testing. These tests are important so that organizations can identify vulnerabilities within their systems. Vulnerability scanning involves scanning network ports with the tool returning possible vulnerabilities and solutions. This allows administrators to be more proactive to network port weaknesses. Password cracking checks the strength of user passwords. Hackers may try to force their way into a

system by trying to guess a user's password, which can happen more easily with weak passwords. By checking user passwords, organizations are proactively trying to prevent attacks. Penetration testing (aka ethical hacking) simulates hacking to identify flaws within the system. Each of these different types of tests can be performed to provide feedback about the security of the network.

Technology, software, and hardware solutions

Network firewalls are like the walls of a castle, serving as a defense to keep out the enemy. Firewalls can help prevent attacks on a single entity or an entire network. Laudon and Laudon (2019) define a firewall as "a combination of hardware and software that controls the flow of incoming and outgoing network traffic" (p. 291). Traffic deemed safe will be allowed to pass through, while traffic deemed unsafe will be denied access. Firewalls are an essential line of defense, but they must be continually maintained rather than implemented and forgotten. Harvey (2018) suggests ten best practices for firewall rules. Those suggestions include using automation to update firewall settings, auditing firewall logs, and updating software and firmware. It is imperative that any updates to the security software be implemented immediately. Holes in security provide an opportunity for cyberattacks.

Imran et al. (2015) describe the qualities of a good firewall as follows: (1) incoming and outgoing information must be filtered by the firewall, (2) the firewall will permit only authorized passage, and (3) the firewall is strong enough to prevent Trojan or phishing attacks. While these are certainly good and necessary qualities of a firewall, to be a successful security measure, a firewall must be accompanied by consistent information systems protocol. Other security measures must also be taken to complement and supplement the firewall security. Firewalls might serve as the first line of defense, but they should never be the company's only defense.

Like any technology, firewalls have evolved since their inception. Next-generation firewalls (NGFW) are the latest in firewall protection. NGFWs offer and can integrate new features such as deep packet inspection, intrusion detection, and inspection of encrypted data (Greene & Butler, 2019). Financial institutions must evaluate their security needs and determine if their firewall technology is current and qualified to face the imminent threats.

There are practical considerations and criticisms with firewall use. Greene and Butler (2019) point out companies need to look at the data capacity supported by the firewall. An important question is whether there are enough servers to support business needs. While some complain firewalls can slow the movement of data, having adequate servers will provide a good balance to this problem. To provide the most up-to-date technology, security, and processing capabilities, companies should assess their current capacity to determine if additional servers are needed.

According to Greene and Butler (2019), intrusion prevention systems and deep packet inspection are important technology pieces that can be included in the firewall or may be standalone. They explain that signature tracing and anomaly detection are a step up from previously used technologies, and deep packet inspection technology may be used to prevent sensitive information from leaving the company's network. As technology becomes more sophisticated, so do the cyberattacks. Companies must keep their systems up to date in order to thwart attacks.

An intrusion detection system, used by firms to provide network protection, can be compared to a home security system. It offers full-time monitoring of the network with tools placed at strategic points (Laudon & Laudon, 2019). The system will produce an alarm or warning if a threat is detected. An intrusion detection system is capable of many tasks including reporting data alterations and errors in the system

configuration (Rozenblum, 2021). It cannot, however, compensate for weak identification and authentication measures, weaknesses in network protocols, or scan everything on a busy network. Intrusion detection systems should be an integral part of a network security protocol. Comprehensive security measures should go beyond just implementing one aspect of technology.

Antivirus software is another defense against cyberattacks. While there have been suggestions in the industry that antivirus software is becoming a thing of the past, the simple reality is, the technology is evolving beyond the traditional personal computer. Antivirus software is still an important part of protecting networks. According to Laudon and Laudon (2019), antivirus software is generally effective in thwarting *known* attackers; this reality makes frequent software updates a necessity. Antivirus software may not be effective against new threats. This underscores the need for multiple levels of security. McMillan (2012) says that antivirus software is still a necessity because it may be required by industry regulations, and it also provides some protection from employees who are naive in their Internet habits (e.g., clicking on certain links or downloading malicious files). Antivirus software will not be effective against all threats, but it is an added layer of security.

As noted earlier, vulnerability scanners are another software option for corporations. The software actively looks for areas that are vulnerable to attack. The scanner can classify vulnerabilities as critical, major, and minor. Beyond this, some upscale products provide penetration testing and patch management. As there are several options for vulnerability scanners, the scanning accuracy and cost should be key considerations for the business.

Limiting access to data is another important measure financial institutions can take to help protect sensitive information. Access controls should be in place to prevent those who are not authorized from gaining access. It is imperative to realize not every employee within a business needs access to *all* information. Authentication software can help businesses manage who is able to access information, and the intent is to ensure that the appropriate information is only accessed by authorized individuals. There are several authentication mechanisms used, including passwords, tokens, smart cards, and biometric screening (Laudon & Laudon, 2019).

Passwords have been used extensively for quite some time, and there have been clear problems with this authentication. Individuals may forget passwords or share passwords. When passwords are easy to guess, this opens the door for cybercriminals. Businesses are making strides in security, and passwords are often required to meet certain criteria, such as length (8-12 characters), number inclusion, and symbol inclusion. This approach helps prevent a brute-force attack by making it harder for a cybercriminal to guess and would take a significant amount of time to crack. Laudon and Laudon (2019) point out two-factor authentication helps overcome some of the problems associated with traditional passwords. In addition to a password, another form of authentication is required to gain access. For an email account, this secondary factor may include a password and a code sent to a personal phone for entry. Without both identifiers, access would be denied.

Biometrics is an automated method for recognition based on some characteristic, generally physical or behavioral (Kalyani, 2017). The various types of biometrics are important in security because they provide a unique identifier. For instance, mobile banking smart phone applications may now include a biometric screening requirement such as the scanning of a fingerprint, which is unique to the individual. Kalyani (2017) goes on to say, “Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods…” (p. 1).

Encryption is another important security feature used to protect data. Laudon and Laudon (2019) define encryption as "the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver" (p. 293). If someone other than an intended party were to intercept the data, they would not be able to understand the content; it is like sending messages in code. While encryption is an important measure, it does not come without challenges, and cloud storage security is one concern. The encryption key must be stored separately from the data. Just as one should not place a house key under the front door mat, the encryption key should not be easily accessible. There is much room for improvement in protecting stored data and it is suggested that data should be encrypted at the point of creation.

The transport layer security (TLS) protocol goes hand in hand with encryption and is generally considered an improvement over the Secure Sockets Layer (SSL) protocol. TLS allows the server and client to authenticate one another via a "handshake," and it prevents third-party interference. As with most technology, improvements to TLS are ongoing. TLS 1.0 was standard for years followed by TLS 1.1 and TLS 1.2. By 2018 healthcare and financial firms are required due to government regulations to update their technology to at least TLS 1.1. For many other industries, upgrading remains optional, although failure to do so is not wise. While regulations help, firms should not wait to update technology until it is absolutely required. By the time the regulation goes into effect, new and better technology is available. Technology has progressed and surpassed businesses and regulations. TLS 1.3 is now available, and Jackson (2021) touts speed and security as being the major enhancements of TLS 1.3 over TLS 1.2. Improvements to security technology are ongoing; it is incumbent upon financial firms and others to implement the technology in a timely manner for the optimum protection against cyberattacks.

Discussion

Based on the critical analysis of the pertaining literature, a set of best practices, presented in Table 1, has been established to help financial institutions prevent as well as recover from network security attacks. These guidelines are designed to help financial institutions ensure that they have accounted for various possible threats, have a plan in place to prevent security breaches, and are prepared to respond to cybersecurity breaches. It is important to note that these guidelines are not hardware or software specific, but rather are a set of directional strategies to help organizations think through their security practices and plans. These items do not have a rank of importance, as each item in the best practice list is equally as important as the next in preventing and mitigating cyberattacks.

Table 1. Financial Industry Best Practices for Cybersecurity

Number	Best Practice
1	Do not rely on a single security measure, but instead use a multi-layered approach.
2	Data should be backed up frequently to limit susceptibility to ransomware threats.
3	Software should be updated frequently to provide maximum protection.
4	Biometric screening should be incorporated into security protocol when possible.
5	Act quickly to minimize the damage when an attack has occurred.
6	Educate staff and users about potential threats.
7	Review security strategies frequently.
8	Have a response plan for security breaches.

Some of the best practices in Table 1 can be grouped together, as they are more technical in nature. It is important to have a breadth of security layers in an organizational security structure. Implementing multiple layers in organizational security means there are several protection barriers for an attacker to

navigate before being able to harm an organization's data or network. Having data backups is important to negate the risks of ransomware attacks. If an attack does happen, the organization can repair the vulnerability and reset the compromised system with little impact to the business. Another important technical factor is to update software frequently. It is impossible for software to be completely flawless, but, as vulnerabilities are discovered or technology changes, companies should release updates to correct security issues as soon as possible. Biometric screening will also help ensure that systems are more secure, as this authentication is less likely to be imitated or hacked. Biometrics should be used with systems containing very sensitive and confidential information. Each technical planning aspect is crucial for a financial institution's success in preventing a network security breach.

Other best practices listed in Table 1 are related to organizational processes, and although not technical in nature, are just as important. These processes are more people oriented. Financial institutions should develop a response plan in the event a cyberattack does occur. In an ideal world, the organization would never have to implement this plan, but a plan does more than just define steps in responding to an attack. While an organization formulates its response plan, it will be reviewing its potential vulnerabilities, which will provide it with opportunities to fortify weaknesses before an attack can occur. Another business process that organizations should implement is ongoing employee training and education about cybersecurity threats. Employees should understand the possible network security threats they themselves can pose to the system. In doing so, organizations can help prevent attacks like malware and ransomware that are often introduced by employees. For financial institutions, this is also important because of the sensitive information to which employees may have access and could accidentally or purposefully expose. Organizations should also review their security strategies frequently to ensure continued success in preventing cyberattacks. As technology changes, so will the requirements for an organization to prevent cyberattacks. This review is both technical and business process oriented. Each of these areas is imperative to help financial organizations keep their systems and data safe.

The last area of focus is responding to an attack, if one should occur. If a network breach were to happen to an organization, it should act quickly to minimize the damage. Acting quickly will allow organizations to keep the trust of their customers, and mitigate further damage resulting from the security compromise. This should include actions like repairing the vulnerability, updating the security plan, as well as releasing a public statement to reinforce customer confidence in the business. A slow response can be detrimental to company outcomes when a plan is not in place to deal with a cyberattack incident. This is especially important for financial institutions because their response in these situations can cause a shift in customer perception and number of customers if the situation is handled poorly. While planning ahead may not account for all necessary decisions to be made, it will certainly ensure that the organization can respond promptly and thoroughly.

Sherry (2014) suggests that organizations should use threat intelligence to battle against cyber attacks. He defines threat intelligence as "an automated process that closely analyzes network traffic seeking to identify the slightest anomaly that could suggest something is amiss" (p. 93). He maintains that "thorough threat intelligence can be an invaluable tool in an overall arsenal to guard against a targeted threat that could potentially cause irreparable harm to an organization's reputation" (p. 94). Moving ahead, he concludes: "Preparedness, rather than reactionary fear, will serve every organization well in addressing cyber vulnerabilities with threat intelligence. Executing it responsibly with financial and technology resources puts businesses in a position to be successful consistently. The advent of aggressive targeted attacks makes these measures a necessity" (p. 94). Furthermore, Hult and Sivanesan (2013) suggest that organizations should go beyond just meeting compliance with information security standards and IT security control frameworks; they should become cyber resilient. They also described the journey from compliance to cyber resilience as "a journey to achieve acceptance of cybersecurity as a key strategic

business-enabler, mission integration across functions to increase agility and performance, a strong focus on skills and experiences driving technology forwards (not vice versa) and the proactive embrace of a threat intelligence-driven approach to defending the enterprise" (p. 124).

Figure 1 illustrates different areas of cybersecurity planning focus, each being equally as important. For businesses that may lack the technical aspects of cybersecurity, the response plan becomes less of an emergency plan and turns into a normal business process due to the constant need to implement the plan. The organization will spend more time responding to these incidences than trying to conduct their normal business. Conversely, if the response plan is missing, the organization will be unable to respond quickly and thoroughly to any breach that may occur. It is important to apply aspects from each area for financial institutions to prevent and respond to these attacks. Each area works together to form a more complete picture of cybersecurity for financial institutions. Figure 1 also shows how each focus area is interrelated and used to improve upon the other. The response plan is implemented after a cyberattack, and the lessons learned from the cyberattack are used to improve upon an organization's technical and business process plans. The technical aspects should be reviewed in order to correct any system or software vulnerabilities. The post-attack internal inquiry would also scrutinize the response plan. The plan would be revised in order to improve upon the action items needed to carry out an effective cyberattack response. Likewise, security strategy, staff education materials, and training curriculum should also be reviewed and updated in order to prevent any future attacks of a similar nature.

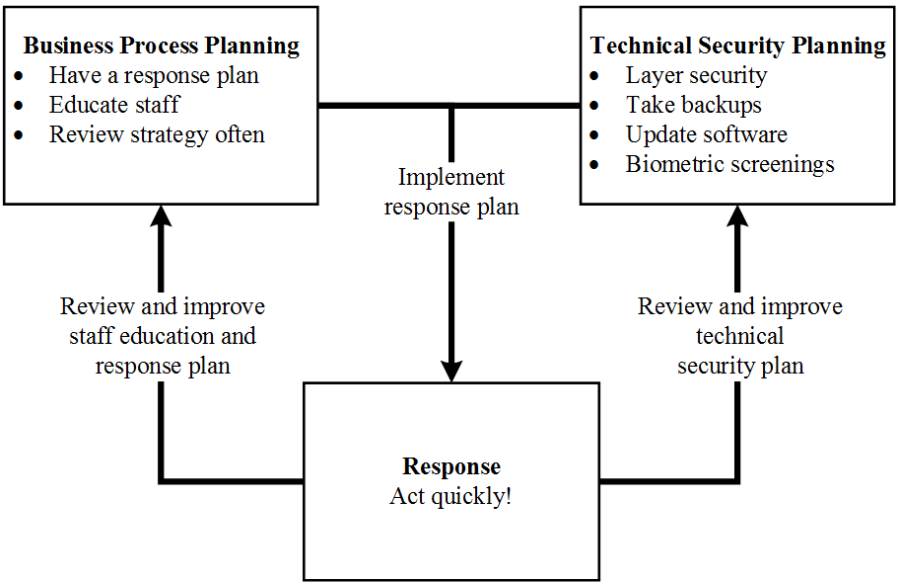

Figure 1. Focus Areas for Preventing and Mitigating Cyberattacks

While reviewing the best practices presented in Table 1, it is important to note that a financial institution's cybersecurity strategy will often differ between companies. There is no one-size-fits-all strategy because each company's resources and priorities will vary. The guidelines in Figure 1 are intended to highlight ideal general practices that all financial institutions should be able to implement in some form. Future research studies may aim to identify specific software or hardware offerings or targeted organizational policies that are superior in providing more concrete guidance to financial institutions. The research approach could entail looking at various financial institutions' user training programs, the security software and hardware employed, as well as their response plans to discover a commonality between organizations which have had success in preventing a cyberattack and those which have not. In doing so, financial institutions should be able to review the outcomes and develop a plan to evaluate internal

security effectiveness. As a result, firms may identify areas of strength and weakness and implement a firm-specific strategy for improvement.

Conclusions

In this paper, we attempt to accomplish two major goals. The first goal is to guide future research. Provided is a critical analysis of cyberthreats, industry practices, and current systems security technology. Utilizing this information, a series of "Financial Industry Best Practices for Cybersecurity" is proposed. These can be used to facilitate future studies. While the focus of the paper is on the financial industry, these best practices can easily be applied across a spectrum of businesses.

The second purpose is to encourage financial industries to adopt procedures and technology to thwart and manage a cyberattack. These proposed best practices can help guide information systems and business executives in developing a systems security plan. As the reliance on technology expands, new threats are mounted. Firms must remain vigilant and new technology must be deployed. Cybercriminals are becoming more sophisticated in their attacks and businesses must stay ahead of the curve. While a great deal of planning and expense go towards preventing a cyberattack, the risk of remaining complacent is often far greater.

The threat of a cybersecurity attack is ever-present and financial firms are at significant risk. Firms must be aware of the threats, have processes in place to address security, and use technology that complements the business processes. For the financial firm, an evolving, comprehensive security plan is the cornerstone of information systems security.

References

Black, P., Gondal, I., & Layton, R. (2018). A survey of similarities in banking malware behaviours. *Computers & Security*, *77*, 756-772.

Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2), 196-200.

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, *32*(1), 63-71.

Fathi, S. (2016, February 3). Managing a hack: A communicator's guide to cyberattack response. https://www.iabc.com/managing-a-hack-a-communicators-guide-to-cyberattack-response-2/

Greene, T., & Butler, B. (2019, January 25). Types of firewalls: What they do and what they're use for. https://www.networkworld.com/article/3230457/lan-wan/what-is-a-firewall-perimeter-stateful-inspection-next-generation.html

Habersetzer, V. (2013). Real-world cyberthreats. *Financial Executive*, *29*(6), 65-66.

Harvey, C. (2018, February 2). Fine-tuning firewall rules: 10 best practices. https://www.esecurityplanet.com/network-security/finetune-and-optimize-firewall-rules.html

Hult, F., & Sivanesan, G. (2013). What good cyber resilience looks like. *Journal of Business Continuity & Emergence Planning*, *7*(2), 112-125.

Imran, M., Algamdi, A. A., & Ahmad, B., (2015). Role of firewall technology in network security. *International Journal of Innovations & Advancement in Computer Science*, *4*(12), 3-6.

Jackson, B. (2021, January 28). An overview of TLS 1.3 - Faster and more secure. https://kinsta.com/blog/tls-1-3/

Kalyani, C. H. (2017). Various biometric authentication techniques: A review. *Journal of Biometrics & Biostatistics*, *8*(5), 371.

Laudon, K. C., & Laudon J. P. (2019). *Essentials of management information systems* (13th edition). Boston, MA: Pearson.

McMillan, R. (2012, March 2). Is antivirus software a waste of money? https://www.wired.com/2012/03/antivirus/

Neville-Neil, G. V. (2017). IoT: The Internet of terror. *Communications of the ACM*, *60*(10), 36-37.

Newman, L. H. (2018, July 9). The worst cybersecurity breaches of 2018 so far. https://www.wired.com/story/2018-worst-hacks-so-far/

Rozenblum, D. (2021). Understanding intrusion detection systems. https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337

Sherry, J. D. (2014). How can threat intelligence help the battle against cyber attacks. *Financial Executive*, *30*(4), 93-94.

Shoorbajee, Z. (2017, September 20). FedEx attributes $300 million loss to NotPetya ransomware attack. https://www.cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack/

Simon, J. D., & Murphy, E. A. (2017). Cybersecurity regulation for financial services companies: New York state leads the way. *Journal of Taxation & Regulation of Financial Institutions*, *30*(4), 27-36.

Tauwhare, R. (2016). Improving cybersecurity in the European Union: The network and information security directive. *Journal of Internet Law*, *19*(12), 3-11.