The State of Cybersecurity in Financial Services

A bluedog Whitepaper

bluedog
SECURITY MONITORING

The State of Cybersecurity in Financial Services

Executive Summary

Security experts working in the financial industry are experiencing even more exacting demands. They now have to defend their organizations in an even faster-changing landscape. The cyber pandemic[1] brought about by the COVID-19 crisis has re-written the rules of the game for everyone, but especially for companies in the financial industry.

More and more attackers are taking advantage of the digitalization of financial institutions, which gives them access to incredible amounts of data. Remote working has also given way to new means of attacks and has made insider-led attacks top-of-mind in the financial industries. Furthermore, there are brand-new challenges around rethinking collaborative practices and company culture as all organizations in the financial sector seek to outmaneuver the uncertainty of the future.

While it seems that the cards are stacked against players – big or small -- in the financial services sector, it's worth noting that for every new threat or risk there is a protective measure that can be applied. Yes, cyber-attacks are growing more sophisticated by the minute, but so are the defenses against them.

This whitepaper will show why financial institutions are more susceptible to cyber-attacks by outlining the most significant cybersecurity statistics from the past few years. The following chapter will focus on the specific threats that financial services companies have to tackle. Lastly, we'll discuss the best approach to mitigate risks in this industry and provide expert recommendations.

[1] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html, retrieved March 2021

Contents

Cybersecurity in Financial Services Statistics

Financial services companies have always been the top targets for cyber-attacks. After all, they hold the money, so it's only natural that banks and other financial institutions are just as attractive to cyber-thieves as El Dorado was to gold seekers.

Even more, financial institutions store a lot of PII (Personal Identification Information) – from name and address to ID cards numbers and even cryptocurrency portfolios, wallets, and credentials. All of these are extremely valuable, so cybercriminals attempt attacks like phishing to compromise the account credentials and gain access to the account or simply get the data they can sell.

While it's not surprising that financial institutions are the favorite target of cybercriminals, the numbers are staggering. It looks like they are 300 times more likely to be targeted by an attack[2] than companies in other sectors. The IBM X-Force Threat Intelligence Index[3] paints a clearer picture: 19% of the total cybersecurity attacks in a year are on a financial institution.

This is why in an annual survey conducted by The Conference of State Bank Supervisors (CSBS)[4], 70% of respondents (managers in community banks) ranked cybersecurity as a top concern. The same survey revealed that only 4% of respondents think that investing in cybersecurity would negatively impact their profitability, while 60% said that they plan to prioritize it.

We agree that prioritization of cybersecurity is a must-have, especially since 70% of financial institutions[5] experienced a security incident in the last 12 months. The leading cause of the attacks was the employees' failure to follow security protocols. This supports what we already knew before the pandemic: employee negligence is the biggest threat to corporate security[6]. Another reason that contributes to the increase in attack frequency is the introduction of the BYOD (Bring Your Own Device), which opens more entryways for cybercriminals. 32% of the attacks can be pinned on BYOD, while 25% are related to file and image downloads, and 24% are accounted by employees sharing data unintentionally.

---

[2] https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth.aspx, retrieved March 2021
[3] https://www.ibm.com/security/data-breach/threat-intelligence, retrieved March 2021
[4] https://www.csbs.org/community-banker-concerns-shift-funding, retrieved March 2021
[5] https://www.darkreading.com/attacks-breaches/70--of-financial-companies-suffered-a-cybersecurity-incident-in-the-past-12-months/d/d-id/1335541, retrieved March 2021
[6] https://businessinsights.bitdefender.com/employee-negligence-remains-the-biggest-threat-in-data-breaches, retrieved March 2021

Deloitte[7] points out that companies in the financial sector spend 0.3% of their revenue and 10% of their IT budget on cybersecurity alone. American Banker[8] shows that big financial institutions and banks spend even more – up to $3000 per employee. However, the Deloitte report emphasizes that money alone and budget increases aren't the solution. Planning and executing security policies are crucial.

According to International Data Corporation (IDC)[9], worldwide spending on security solutions is expected to reach $151.2 billion by 2023. The research report shows that this number is largely supported by financial institutions, who will shed 35% of their budget on the mitigation of cyber risks.

If you think that financial institutions spend too much on cybersecurity, then you have to see the cost of a successful cyber-attack. This cost is, of course, highest in the financial industry can it can reach $18.3 million[10]. Yes, that is a single successful attack on a single financial company.

Ponemon Institute[11] surveyed 400 security professionals in the financial services industry to find out that 56% of think they are good at threat detection, but only a little over 30% are also good at threat prevention.

This is quite a problematic approach and part of the reason why so many attacks are successful. Mastercard[12] says that they deal with 400,000 breach attempts every day! Granted, they are one of the biggest companies in the industry but this doesn't mean that smaller companies are completely out of harm's way.

Now that we've seen why prioritizing cybersecurity is crucial for companies in financial services, let's take a look at the threats they are faced with most often.

---

[7] https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html, retrieved March 2021

[8] https://www.americanbanker.com/articles/financial-firms-spend-up-to-3-000-per-employee-on-cybersecurity, retrieved March 2021

[9] https://www.businesswire.com/news/home/20191016005057/en/New-IDC-Spending-Guide-Sees-Solid-Growth, retrieved March 2021

[10] https://www.accenture.com/us-en/insights/financial-services/cost-cybercrime-study-financial-services, retrieved March 2021

[11] https://www.prnewswire.com/news-releases/synopsys-and-ponemon-release-new-study-highlighting-software-security-practices-and-challenges-in-the-financial-services-industry-300894781.html, retrieved March 2021

[12] https://www.nytimes.com/2019/07/30/business/bank-hacks-capital-one.html, retrieved March 2021

Top Threats in Financial Services Cybersecurity (and How to Mitigate Them)

Recognizing the problem is the first step in knowing how to deal with it. Many financial institutions aren't' sure about where to start. The cybersecurity landscape is, indeed, a very vast one. But a good first step is knowing which the most common threats a financial services company might face are.

You can then conduct risk assessment and vulnerability scans to quantify your company's specific risks and create a plan to mitigate them.

Malware

The term "malware" refers to malicious software or code snippets that can be introduced in the company's system through:

- Email attachments
- Removable media (like flash drives)
- Downloads from malicious websites posing as legitimate ones

Malware attacks are very dangerous because they can harm you in more ways than one. For instance, they can compromise the integrity and confidentiality of customer data (which is often very sensitive data in financial companies. They can also destroy that data or disrupt your systems and render your business inoperative.

You can prevent malware attacks from being successful through a few simple steps:

- Train your employees to recognize potential issues (fraudulent websites or suspicious email attachments).
- Make the scanning of email attachments mandatory.
- Place restrictions on using removable media devices.
- Make sure that all the devices and systems are updated with the latest security patches.
- Create a strict BYOD policy.
- Implement a network monitoring policy which will immediately identify calls made from software to known compromised IP address and Command and Control servers.

Phishing and Business Email Fraud

A phishing attack happens when attackers create and send emails that seem legitimate to company staff members or to customers in order to trick them into revealing sensitive personal information like login credentials or into sending funds.

A common phishing technique is impersonating a company's CEO or other executive and instructing a client to transfer funds in exchange for a substantial reward. Another common technique is impersonating an official account (customersupport@financialinstitution.com) and asking the client to login to update their information. When they click on the link in the email, they are led to a website that looks and feels like the "original", but is a scam. As soon as the user enters their credentials, the hackers will have access to them.

You can minimize the risk of phishing attacks by training your personnel to spot phishing attempts and adding additional control policies, like the obligation to confirm any wire transfer by phone.

Once again, carefully managed network monitoring, by trained SOC analysts will quickly alert you of any attempts by your employees to access sites with malicious content; which is of course the intention of the phishing operators. The sooner you can be alerted, the less damage will be done.

Ransomware

Ransomware is a form of malware that encrypts the files in your system and demands a ransom in exchange for the encryption key you need to unlock your files. This is a very common threat for financial services companies and a very serious one.

A ransomware attack will render your business inoperative and seriously damage your reputation. This is why it's important to prevent it rather than to deal with it when it happens.

In order to minimize the risk of a ransomware attack being successful, you should train your personnel to access internet files and websites only if they are trusted. More importantly, you should have thorough plans for business continuity and incident response in place.

Distributed Denial of Service (DDoS)

In this type of attack, the hacker typically uses bots or similar tools to flood the company's servers with internet traffic. This results in slowing down or completely shutting down the traffic from legitimate users. Consequently, your business may be rendered inoperative or simply be very hard to access.

Attackers who use the DDoS technique can be politically motivated or they may use DDoS as a way to mask another type of attack. While you are busy solving the DDoS downfall, they can escape with your customers' sensitive data or create another type of breach.

To mitigate the risk of a successful DDoS attack, you have three techniques at your disposal:

- Constantly monitor website traffic and flag any spikes that aren't easily explainable.
- Develop a strong incident response plan.
- Consider using third-party services to manage your internet traffic.

Watering Hole

The Watering Hole technique is one of the more recent types of attacks that target financial institutions. To perform such an attack, the cybercriminals typically identify a less secure website that is regularly visited by your employees – it can be anything from online shops to the food delivery service that's used in your office regularly (hence the name "Watering Hole").

The attacker infects that website with malware in the hope that, this way, your employee's computer might become infected as well. Thus, they would gain an entryway to your company's system and access to your data.

To minimize the risk of a Watering Hole attack:

- Monitor website traffic.
- Inspect the websites regularly visited by your employees for malware.
- Block any infected websites your inspection may uncover.
- Keep your systems up-to-date and ensure that your employees use updated and properly configured browsers.

- Regular automated VAPT scanning will pin-point weaknesses in your defenses which cybercriminals will use to attack your systems.

Take the Proactive Approach to Security

As the statistics in the first chapter show, very few financial institutions take prevention seriously. The steps above are great for mitigating each individual risk, but you need a more comprehensive plan to tackle your security as a whole.

The cybersecurity landscape evolves and changes every day and the same has to happen to your cybersecurity strategy. Bluedog Security Monitoring services have been designed with financial institutions in mind; Regular VAPT, Managed Detection and Response[13] and virtual CISO[14] are just a few. We can help you go beyond compliance and get the peace of mind you and your clients need.

[13] https://bluedog-security.com/managed-detection-and-response/, retrieved March 2021
[14] https://bluedog-security.com/virtual-ciso/, retrieved March 2021

About Bluedog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@bluedogsec.com

+44 20 8819 6254