Future of Risk

Financial services firms have a lot to lose from cyberattacks

May 18, 2022

All businesses are at risk of ransomware and other attacks, but financial services firms have more at stake.

By Stan Bernard, Head of Financial Institutions and Professional Services, U.S. Middle Market, Zurich North America

As both the number and financial toll of cyberattacks continue to climb, financial services businesses remain among the top targets of cybercriminals. According to one report, the banking industry experienced 15,537 ransomware attacks during in the first half of 2021, more than government, manufacturing, healthcare, or food and beverage sectors.[1] Another estimate notes that the average cost of a data breach in the financial sector was $5.72 million in 2021.[2] Indeed, Federal Reserve

Chairman Jerome Powell warned that cyberattacks are the top threat to the global financial system.[3]

For financial services firms, whether depository institutions, asset managers, insurance companies or other organizations, the severity and potential consequences of a successful network intrusion, data theft or ransomware attack can be costly, far-reaching and long-lasting.

High-value targets

There are obvious reasons why financial services businesses are at such elevated risk. All such businesses maintain huge databases of highly sensitive, personally identifiable information that can be leveraged and monetized by cybercriminals. From credit cards and deposit information to estates, wills, titles and other critical data stored electronically, financial firms are prime, high-value targets for criminal activity. Additionally, the lure of an institution perceived to be flush with cash motivates many hackers to target local banks and credit unions they believe may have fewer cyberdefenses than large, money-center banks. Sadly, they are often correct.

The reputational and customer confidence impacts of a successful cyberattack are just part of the story. Regulatory bodies may also impose costly, post-event reporting requirements as well as significant fines for failing to keep personal data reasonably protected. And while reporting requirements for ransomware attacks not associated with personal data theft are not as stringent, that only means that there may be many more of these types of attacks than widely reported in the mass media.

Bottom line: If you manage a financial services business of any size and type, when it comes to cybercrime, you have a target placed squarely on your back for ransomware, data theft and other threats.

Five top cyber risks facing financial services

According to an industry fraud protection specialist, these are the top five cyber vulnerabilities threatening financial services firms:[4]

1. Unencrypted data

All data stored on a financial institution's network should be encrypted. If not, cybercriminals can disseminate and monetize that data as soon as it is acquired.

2. Malware from end users

End-user devices that have been compromised, such as computers and cellphones belonging to account holders, can pose a direct risk to a firm's network.

3. Unsecure third-party services

Many financial institutions employ third-party services to enhance customer service. If vendors don't have good cybersecurity, the institution may be at risk.

4. Data manipulation

Sometimes hackers don't steal data; they simply corrupt it. Since altered data and codes may not appear or function substantially differently from unaltered, it may be very difficult to detect this kind of attack.

5. Spoofing

Spoofing is the act of hackers impersonating an institution's website's URL with a fake site that looks and functions in the same way. The threats to users and the institution are obvious.

Building a culture of cybersecurity

Employee training addressing email phishing, social engineering and password management is fundamental in an environment of heightened cyber risk. Human factors and behaviors continue to present the greatest risks in any information security framework. These can be minimized by ongoing training, coaching and periodic testing, such as “dummy” phishing attempts to determine whether employees are on their games when it comes to security awareness.

It is also important to enable automatic updating for all your devices. Cybercriminals are constantly looking for new vulnerabilities in devices and software. Keeping IT resources automatically updated will help ensure known weaknesses are patched and otherwise addressed on all devices as soon as software providers release fixes.

In addition, a growing number of organizations are employing the following processes and procedures as table stakes in the battle against increasingly aggressive and costly cyberattacks:

- **Multi-factor Authentication (MFA)** – This authentication strategy requires users to provide two or more verification factors to gain access to a network, application, online account, VPN, file or other IT resource. Rather than simply requesting a username and password, MFA requires a unique, time-limited numeric code and sometimes additional verification factors to allow access.
- **Privileged Access Management (PAM)** – This security protocol includes policies, strategies and technologies used to control, monitor and secure elevated access to critical resources. PAM strategies include the “principle of least privilege,” which restricts account creation and permissions to the minimum level a user requires to perform job responsibilities.
- **Security Operations Center (SOC)** – Network security can be enhanced by a dedicated SOC, whether within the organization or provided as a service. An SOC is a centralized function employing people, processes and technology to continuously monitor an organization's security posture.
- **Security & Awareness (S&A) Training** – An estimated 90% of breaches are made possible when someone falls victim to a phishing email (according to CISCO’s 2021 Cybersecurity Threat Trends report). Security & Awareness training is essentially education of employees and other end users to better understand the risks posed by phishing and other social engineering techniques.

- Cloud backups with tested recovery – Most organizations recognize the need to back up their data and applications, but equally important is ensuring they are capable of using those backups to recover from an incident. Recovery testing is exercising the organization's disaster recovery plans to reliably retrieve data should the need arise.

Before and after a cyberattack

While the cyber defenses of many financial services businesses have been strengthened in recent years, even the best defenses can be circumvented by today's breed of cybercriminals. This is no time for overconfidence because the tools available to bad actors are evolving and becoming more insidious by the day.

Pre-event – Recognizing that the threat is constantly evolving, adopt and maintain a proactive defense strategy based on the standards of NIST[5] or recommendations by the federal government's advisory program.[6] Perform regular inspections and vulnerability assessments to stay on top of evolving cybercrime tactics, and make sure you are not relying entirely on any one defensive technology. A multi-layered defensive posture will be your best deterrent, including strong detection and interception capabilities.

Post-event – If, no matter how thoroughly you prepare, your firm becomes the victim of a network intrusion or ransomware attack, your formally documented response plan should be activated immediately. Your plan should contain contact information to activate your designated breach coach and any other forensic assistance you may require. It should also contain detailed instructions regarding notification requirements for all relevant jurisdictions — including any federal authorities noted in the plan — and the level of reporting required.

In short, have a plan that has all the elements you may need in the event of a successful cyberattack, including detailed business continuity plans to continue operations during the crisis. You should also have a tested network recovery plan, including “air-gapped” data backups — i.e., backups completely isolated from the main network — updated and held in a secure location for rapid access.

In conclusion, the global pandemic of cybercrime, with evermore contagious and malicious variants of ransomware posting to the dark web every day, will not slow anytime soon. There is no vaccine for the next malicious virus or strain of malware headed your way other than your own vigilance, planning and determination to protect what is most valuable to your business and reputation. Building cyber resilience against this evolving threat can only happen through awareness, training and employee commitment.

For additional information about developing cybersecurity threats, you may want to follow updates from the federal Cybersecurity & Infrastructure Security Agency (CISA). And for information about how Zurich can help you protect your network, data and IT resources, learn about Zurich Cyber Risk Engineering Services.

1. “Attacks from All Angles: 2021 Midyear Cybersecurity Report.” Trend Micro. 14 September 2021.
2. IBM Cost of a Data Breach Report. July 2021.
3. Fung, Brian. “Cyberattacks are the number-one threat to the global financial system, Fed chair says.” CNN Business. 12 April 2021.
4. “The 5 Biggest Threats to a Bank’s Cyber Security.” SQN Banking systems.
5. “The Five Functions.” NIST Cybersecurity Framework. 12 May 2021.
6. National Cyber Awareness System. Cybersecurity & Infrastructure Agency (CISA).

https://insights.zurichna.com/Financial-services-firms-have-a-lot-to-lose-from-cyberattacks