FACTSHEET

Common Areas of Risk in the Financial Services Industry

DID YOU KNOW?
In 2017, more than 24,000 records were compromised in an average data breach.[1]

With so many records at risk, businesses across North America must be aware of their areas of vulnerability.

Denial-of-Service (DoS) attacks

DoS attacks, including distributed denial-of-service (DoS) attacks and DoS botnet attacks, are the most common types of scams affecting the financial service industry.[2] Cyber criminals flood a network or machine with traffic or send information to trigger a crash and deprive users, such as account holders of services.

Digitization

Bank and financial service providers are increasingly engaging customers online or through mobile phones and Internet of Things (IoT) devices. But some network-connected devices are not always secure.

Phishing scams

A Business Email Compromise (BEC) scam is one of the most common scams used to try to trick victims out of money and confidential financial data. A criminal gains access to a corporate email account and then spoofs the owner's identity to defraud the company.

Cyber criminals

The top external threat facing the financial services industry are cyber criminals (40%) followed by nation-states (18%), 'hacktivists' (16%), and business competitors (13%).[6]

Financial malware

With more than 1.2 million annual detections, financial malware is a huge threat and 2.5 times more common than ransomware.[4] In an earlier study, 75% of the top 20 U.S. commercial banks were infected with malware.[5]

Dated equipment

Financial services firms are constantly incorporating new technology, systems and software into their operations, and legacy IT systems are often inherited from acquired organizations. But old assets, and stockpiling them, can make the organization vulnerable to attack.

Insiders

In a recent report, 60% of respondents from the global financial industry cited privileged users as the biggest insider threat, followed by executive staff (48%) and contractors (38%).[6] Fraudulently transferring money, or using personal information of customers for identity theft, are examples of privilege misuse.

Negligent employees

A lot of research has shown that careless employees who don't follow security policies are the biggest security threat in organizations.[7] By sharing passwords openly, carrying sensitive information unnecessarily and leaving mobile devices unattended outside of the workplace, they leave their organizations vulnerable to attack.

Third-party partners

Many financial service providers depend on multiple vendors, partners and other third parties. Studies have shown that approximately 60% of Chief Information Security Officers (CISOs) express some concern about third-party security practices and risk of a data breach.[3]

COMMON AREAS OF RISK IN THE FINANCIAL SERVICES INDUSTRY

3 Tips to Keep Your Business Secure

Identify All Potential Areas of Risk

Conduct a walk-through of your office. Point out and mitigate any risks that you see. This will allow you to discover your pain points and solidify an information security strategy to keep data secure.

Implement Secure Workplace Policies

By establishing comprehensive policies such as a *Shred-it All* Policy and Clean Desk Policy, you encourage people to think twice about their actions in the workplace. This will push them to comply and help protect your data.

Build a Total Security Culture

Using a top down approach and integrating information security throughout the workplace, you will be able to embed it into people's everyday behavior. This will encourage them to re-consider how to securely destroy any and all confidential information.

Sources:

1. 2017 Cost of Data Breach Study, Ponemon Institute, 2017
2. 2017 Data Breach Investigations Report, 10th Edition, Verizon
3. What CISOs Worry About in 2018, Ponemon Institute and Opus, 2017
4. Internet Security Threat Report, Financial Threats Review 2017, Symantec
5. 2016 Financial Industry Cybersecurity, Security ScoreCard
6. 2017 Thales Data Threat Report, Financial Services Edition, Thales e-security
7. Promoting Data Security in the Workplace infographic, University of Alabama at Birmingham; 2016 State of the Endpoint Report, Ponemon

Learn more about information security in the financial services industry:

888-227-0923 | shredit.com/finance

Shred-it® is a Stericycle solution.

Shred-it®