Defending Financial Institutions from Cyber Attacks.

CNA
We can show you more.®

FINANCIAL INSTITUTIONS

Address a Growing Problem with Simple Strategies.

While financial institutions have always been a target for cyber-attacks, recent data breaches have further increased the awareness of their vulnerability. Financial information, while valuable by itself, can also be used for nefarious purposes such as identity theft and account takeover. An attacker armed with a victim's basic information and bank account or credit card number, may be able to convince a customer service representative to alter the victim's account for fraudulent gain. Changing the shipping address on an Amazon account or ownership of a website domain are examples of this common tactic. Security awareness training for employees, securing embedded devices and implementing strong password management practices are three strategies that financial institutions can implement to help reduce security incident severity and frequency.

Your Greatest Asset can be your Best Defense.

A company's employees are among its greatest assets and frequently the front line of defense against cyber attacks. While technologies such as email spam filtering and antivirus are typically utilized to protect an organization, these solutions are never 100 percent effective. Ongoing security awareness training can help ensure that employees are cognizant of common attacks that include spam and phishing emails, as well as social engineering attempts that may affect them in the workplace. This type of training should also address issues such as a clean desk policy, how to report a potential security incident, and maintaining physical custody and control of company assets. Most importantly, this effort should not be limited to a single instance at the time of hire, but should be an ongoing training exercise that occurs multiple times per year. Organizations should consider mimicking phishing campaigns on their employees and use these opportunities for educational growth.

New Technologies Create New Vulnerabilities.

In addition to laptops and desktops used in financial institutions, other equipment is increasingly becoming "smart" and connected. What were once standalone systems with limited functionality are now network connected and run complex operating systems that enable additional services. These devices have become — in reality — computers. And just like laptops and desktops, they have vulnerabilities that require regular security patches and proper configuration to ensure that they do not become the point of entry for a breach. Heating and ventilation systems, badge access systems for door entry and security cameras may now be connected to the internet for remote management. Left unsecured (utilizing factory default settings, for example) these devices become a springboard into the corporate network for attackers. In some cases, security may not have been considered in product design, making it very difficult to protect.

As Security Gets Stronger, Attackers Get Smarter.

Another well-documented issue is attacks against ATMs. While most are aware of the classic "skimming" attack, where a device is placed in front of the card-reading slot and used in conjunction with a camera to capture the PIN as it is entered, these attacks have adapted and increased in maturity as the financial market has attempted to thwart them. Attackers have devised clever ways to insert the skimmer inside the ATM by drilling a small hole near the card reader.[1] They will also leverage known vulnerabilities in ATMs that are running the long-unsupported Windows XP operating system. Here, holes cut in the chassis expose a USB port beneath, allowing attackers to install malicious software and later extract currency while wiping their electronic tracks clean.[2] Finally, with the deployment of more secure EMV cards, attackers are again looking for ways to stay one step ahead. A new device called a "shimmer" has been discovered at ATMs in Mexico. Inserted in the card slot of the ATM, the device "acts as a shim that sits between the chip on the card and the chip reader in the ATM — recording the data on the chip as it is read by the ATM."[3]

Simplify the Process, but Keep the Passwords Complex.

Financial institutions need to ensure that good password policies are implemented in their environments. While seemingly basic, cracking weak passwords is a common method for attackers to access a network and exfiltrate data. Important requirements of a cyber policy include never sharing passwords (for any reason), ensuring that passwords are long and complex, and using unique passwords for each system/application. Unfortunately, human beings are not great at remembering multiple long complex passwords, which is why simple passwords are commonly reused. Organizations can look to technologies such as Single Sign On (SSO) and Federated Identity Management (FIM), as well as password management services, to assist their employees in practicing strong password habits.

Minimize your Exposure and Protect your Bottom Line.

Risk management is addressed through one of four primary principles: acceptance, avoidance, mitigation and transfer. Many of the suggested recommendations discussed in this article fall within the risk mitigation category, and along with acceptance and avoidance, are methods to successfully manage risk in your organization. Organizations may wish to consider transferring risks that cannot be adequately dealt with using one of the other three methods. A cyber insurance policy, such as the CNA NetProtect® product, can assist in managing cyber risks at an acceptable level. CNA NetProtect® offers first-and-third-party coverages associated with e-business, the Internet, networks, and other electronic assets and information. First-party coverage is available for network extortion, business interruption, extra expense, loss or damage to a network and e-theft. Third-party liability includes media liability, privacy liability, network security liability, and costs to comply with privacy breach notification laws and defense of privacy regulatory proceedings.

Nick Graf, CISSP, CEH, CIPT is the Risk Control Consulting Director of Information Security. He has worked in information security for 10 years, specializing in Data Leakage Prevention, Security Policies, Incident Response, Data Breach and Security Awareness. Nick has presented courses on privacy, big data, the cloud and healthcare risks and has also written and contributed to articles including information risks, social engineering, mobile device security, phishing and personal password management. Nick previously worked at HSBC bank in the area of application security, is a Certified Ethical Hacker and holds a Master's degree in Computer, Network and Information Security from DePaul University.

[1] "New ATM Skimmers Connect To The Card Reader Via A Nearly Invisible Hole" Accessed October 15th 2015 http://techcrunch.com/2014/12/01/new-atm-skimmers-connect-to-the-card-reader-via-a-nearly-invisible-hole/.

[2] "Who's Still Robbing ATMs with USB Sticks?" Accessed October 15, 2015 http://www.wired.com/2013/12/whos-robbing-atms-usb-stick/.

[3] "Chip Card ATM 'Shimmer' Found in Mexico" Accessed October 15th 2015 http://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/.

The information, examples, and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual stations. Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect thereto. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice. CNA is a service mark registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities.

Copyright © 2016 CNA. All rights reserved. FI055M