Mobile Banking App is HERE!

UNION BANK

February 2023

Insider threats are a major security issue in the financial sector

Member FDIC

EQUAL HOUSING LENDER

The Financial industry is becoming a hot target for hackers and ransomware, and it's no surprise — the industry does deal with money, after all. The sector is 300 times more likely to experience a cyberattack than any other industry, and the industry is absorbing the highest cost with an average of $18.3 million lost per cyberattack. But it's not just the Scrooge McDuck-style pools of coins and cash that cause hackers to turn their eyes to financial institutions. It's the access. The industry has a vast amount of internal users that can quickly turn into insider threats.

What are insider threats?

An insider threat is simply a cybersecurity threat (the potential theft or compromise of critical data or assets) that comes from an internal user, i.e an employee. While insider threats can happen accidentally or on purpose, they are a threat to be taken seriously. According to the Ponemon Institute 2020 Cost of Insider Threats: Global Study, there were 4,716 insider attacks recorded across the globe, and the cost of an insider incident almost doubled between 2019 and 2020 from $493,093 to $871,686. These incidents can arise from an outside source paying the internal user, the termination gap where a terminated user still has access, or simply when human error comes into play. The financial industry, not unlike the healthcare industry, is rife with insider threats. While there is the obvious threat of those seeking financial gain, the financial industry is also prone to attack from nation-states, rival corporations, and cyber-espionage groups. That's a lot of darts getting thrown at one target.

Why is the finance industry at risk for insider threats?

On average, a financial services employee has access to nearly 11 million files the day they start work. Now expand that number across an organization or multiple organizations of the entire industry. It's unfathomable how many assets full of PII and other sensitive information (like bank account information) is being accessed at any given moment. Securing all those assets becomes a major challenge for financial organizations, and that's not even taking into account SOX 404, GLBA Safeguards Rule, and other regulatory demands. For hackers, it becomes obvious that the fastest way in is through an internal user. Just look at PostBank, the South African post office bank that was forced to replace millions of bank cards at a cost of $58 million after an internal employee compromised customers bank data by copying a master key. That was just a compromise, not a full-fledged theft, and it still cost over $50 million. All it

Continued on Page 2

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

takes is one moment of human error, a moment of weakness, a well-placed phishing attack on an internal user with too much access to cause chaos. Not to mention that as financial institutions, like organizations in every industry, become more digitized and decentralized, they open themselves up to new threats and more vulnerable access points.

How the finance sector can stay safe from insider threats

There are a few building blocks of cybersecurity architecture that a financial organization can place to have a better foundation against mounting threats – both external and internal.

Create access policies that follow least privilege access. Your organization may not know who has access to what assets, but a hacker probably does. With malware, spyware, and other bugs gaining sophistication, it isn't a stretch for a determined back actor to figure out which internal user has too much access and then target them with a phishing attack or straightforward extortion. By never giving a user access to more than the minimum they need to do a task (and then deprovisioning that access after), an organization is preventing access creep and removing a potential attack surface.

Implement fine-grained controls that employ zero trust. The methodology behind access policies apply to access controls — trust no one. Internal users should be beholden to the same controls any external users are, and no one should be above that idea. From utilizing time-based controls to multi-factor authentication, a mix of access controls can prevent an attack before it even occurs.

Conduct regular access reviews. A user access review is a periodic inventory of access rights to certain networks and systems, and the users who have access permissions into those networks and systems. By regularly having IT and HR conduct those reviews, an organization can prevent access creep, the termination gap, or find credentials that were errantly given out. These kinds of reviews can also flag certain insider bad behavior like snooping. User access reviews also help a financial organization meet SOX compliance.

Source: Imprivata

Three Types of Insider Threats

There are three common types of insider threats that financial companies and institutions face.

The first one is an intentional or malicious attack.

This is where some active employee has a grudge against the company, or turns traitor due to financial incentives or for some other reason. Then they use their legitimate credentials to attack the company.

For example, J.P. Morgan Chase's Peter Persaud sold personal identifying information (PII) and PIN numbers to outside parties, and many of the accounts were later targeted. Persaud received a sentence of four years in prison in 2018.

Or there's this case, where TD Bank employee Janelle Digby, a call center representative, worked with co-conspirators to hand over sensitive client information. Another party associated with Digby got people to open new accounts at the bank for the purposes of defrauding the institution and taking money out of the bogus accounts.

The second type of threat is an unintentional attack that can be called "negligent."

Here, employees aren't trying to hack the company, but the outsiders persuade them to turn over information through some kind of deceit or trickery.

How does this work? A telling case involving giant bank HSBC provides some detail. Here's how a reporter put it in coverage at the Royal Gazette in 2017:

"HSBC Bermuda yesterday apologized after it e-mailed personal information on customers to other account holders. The e-mails contained names, e-mail addresses, countries of residence, the name of the customers' relationship manager and HSBC customer identification numbers."

In these types of cases, the latent information can then be used by unscrupulous parties to conduct attacks, which is why HSBC's release was so grievous.

A third kind of insider threat involves recruitment where outsiders get insiders to flip or turn, to accomplish their objectives.

Late in 2021, the US District Court for the Eastern District of Virginia saw three men charged with money laundering and other crimes, in a case where they allegedly sent false emails to an employee so that they could get access to real transaction information. One of the accused reportedly was found to have worked at Bank of America for some time from 2015 to 2018. Coverage of this incident shows how the hackers had to deceive employees close to the banking transactions.

Whether it's a malicious insider attack, a case of negligence, or a recruiting setup, the results are still devastating, so businesses have to be on the lookout for all of these scenarios.

Source: Teramind

12 Simple Things You Can Do to Be More Secure Online

1. Install an Antivirus and Keep It Updated

We call this type of software antivirus, but fending off actual computer viruses is just one small part of what they do. Ransomware encrypts your files and demands payment to restore them. Trojan horse programs seem like valid programs, but behind the scenes, they steal your private information. Bots turn your computer into a soldier in a zombie army, ready to engage in a denial-of-service attack, spew spam, or whatever the bot herder commands. An effective antivirus protects against these and many other kinds of malware.

In theory, you can set and forget your antivirus protection, letting it hum along in the background, download updates, and so on. In practice, you should look it over every now and then. Most antivirus utilities display a green banner or icon when everything is hunky-dory. If you open the utility and see yellow or red, follow the instructions to get things back on track.

One more thing. If your antivirus or security suite doesn't have ransomware protection, consider adding a separate layer of protection. Many ransomware-specific utilities are entirely free, so there's no reason not to try a few of them and select the one that suits you best.

2. Explore the Security Tools You Install

Many excellent apps and settings help protect your devices and your identity, but they're only valuable if you know how to use them properly. To get the maximum protective power from these tools, you must understand their features and settings. For example, your smartphone almost certainly includes an option to find it if lost, and you may have even turned it on. But did you actively try it out, so you'll know how to use it if needed?

Most antivirus tools have the power to fend off Potentially Unwanted Applications (PUAs), troublesome apps that aren't exactly malware but don't do anything beneficial. But not all of them enable PUA detection by default. Check the detection settings and make sure yours are configured to block these annoyances. Likewise, your security suite may have components that aren't active until you turn them on. When you install a new security product, flip through all the pages of the main window, and at least take a glance at the settings. If it offers an initial onboarding tour, don't skip it—rather, go through the tour methodically, paying attention to all the features.

3. Use Unique Passwords for Every Login

One of the easiest ways hackers steal information is by getting a batch of username and password combinations from one source and trying those same combinations elsewhere. For example, let's say hackers got your username and password by hacking an email provider. They might try to log into banking sites or major online stores using the same username and password combination. The single best way to prevent one data breach from having a domino effect is to use a strong, unique password for every single online account you have.

Creating a unique and strong password for every account is not a job for a human. That is why you use the random password generator built into your password manager. Several very good password managers are free, and it takes little time to start using one. For-pay password managers generally offer more features, however.

4. Get a VPN and Use It

Any time you connect to the Internet using a Wi-Fi network that you don't own, you should use a virtual private network or VPN. Say you go to a coffee shop and connect to a free Wi-Fi network. You don't know anything about the security of that connection. It's possible that someone else on that network, without you knowing, could start looking through or stealing the files and data sent from your laptop or mobile device. The hotspot owner might be a crook, sniffing out secrets from all Wi-Fi connections. A VPN encrypts your internet traffic, routing it through a server owned by the VPN company. That means nobody, not even the owner of the free Wi-Fi network, can snoop on your data.

5. Use Multi-factor Authentication

Multi-factor authentication can be a pain, but it absolutely makes your accounts more secure. Multi-factor authentication means you need to pass another layer of authentication, not just a username and password, to get into your accounts. If the data or personal information in an account is sensitive or valuable, and the account offers multi-factor authentication, you should enable it. Gmail, Evernote, and Dropbox are a few examples of online services that offer multi-factor authentication.

Multi-factor authentication verifies your identity using at least two different forms of authentication: something you are, something you have, or something you know. Something you know is the password, naturally. Something you are could mean authentication using a fingerprint, or facial recognition. Something you have could be your mobile phone. You might be asked to enter a code sent via text or tap a confirmation button on a mobile app. Something you have could also be a physical Security Key; Google and Microsoft have announced a push toward this kind of authentication.

6. Use Passcodes Even When They Are Optional

Apply a passcode lock wherever available, even if it's optional. Think of all the personal data and connections on your smartphone. Going without a passcode lock is unthinkable.

Many smartphones offer a four-digit PIN by default. Don't settle for that. Use biometric authentication when available, and set a strong passcode, not a stupid four-digit PIN. Remember, even when you use Touch ID or equivalent, you can still authenticate with the passcode, so it needs to be strong.

7. Pay With Your Smartphone

The system of credit card use is outdated and not very secure at all. That's not your fault, but there is something you can do about it. Instead of whipping out the old credit card, use Apple Pay or an Android equivalent everywhere you can. There are tons of choices when it comes to apps.

8. Use Different Email Addresses for Different Kinds of Accounts

People who are both highly organized and methodical about their security often use different email addresses for different purposes, to keep the online identities associated with them separate. If a phishing email claiming to be from your bank comes to the account you use only for social media, you know it's fake.

9. Clear Your Cache

Never underestimate how much your browser's cache knows about you. Saved cookies, saved searches, and Web history could point to home address, family information, and other personal data.

To better protect that information that may be lurking in your Web history, be sure to delete browser cookies and clear your browser history on a regular basis.

10. Turn Off the 'Save Password' Feature in Browsers

Speaking of what your browser may know about you, most browsers include a built-in password management solution.

11. Don't Fall Prey to Click Bait or Phishing Scams

Part of securing your online life is being smart about what you click. Clickbait doesn't just refer to cat compilation videos and catchy headlines. It can also comprise links in email, messaging apps, and Facebook. Phishing links masquerade as secure websites, hoping to trick you into giving them your credentials. Drive-by download pages can cause malware to automatically download and infect your device.

Don't click links in emails or text messages, unless they come from a source you trust. Even then, be cautious; your trusted source might have been compromised, or the message might be fake. The same goes for links on social media sites, even in posts that seem to be from your friends. If a post seems unlike the style of your social media buddy, it could be a hack.

12. Protect Your Social Media Privacy

There's a common saying: if you're not paying for a service, you're not a customer; you're the product. Social media sites make it easy for you to share your thoughts and pictures with friends, but it's easy to wind up sharing too much.

Source: ***PCMag, Neil J. Rubenking & Jill Duffy, Updated August 29, 2022***