Financial Services

Top 4 Cybersecurity Threats

Going back to basics in financial services.

splunk>

Foreword

There's no shortage of cybersecurity threats to keep Chief Information Security Officers (CISOs) on their toes. In 2023, 94% of financial services CISOs were concerned about their personal liability for cybersecurity incidents — more than any other industry surveyed. And the SEC continues to pressure CISOs to act responsibly. To ease their anxieties, CISOs should focus on preventing the threats that matter most. But where's the right place to start?

I think it's time to get back to basics when navigating cybersecurity threats. While elaborate hacks like cryptojacking, ransomware and spyware are getting a lot of attention, they haven't replaced some of the classics.

In reality, more traditional security threats remain some of the largest concerns for financial services. As the industry continues to digitize and more customers rely on apps to manage their money, the threat landscape continues to grow. Account takeovers, business email compromise, insider threats and social engineering attacks can wreak havoc on their own, and these core attacks can lead to more nefarious cyber threats and means of fraud. And with account takeovers and account abuse making up a majority of financial crime, focusing on traditional cyberattacks can help reduce risk in a big way.

Trust is foundational in financial services. And the need for safe, secure customer data to reinforce that trust is paramount. But financial services institutions are frequently targeted by cyber threats, which can lead to serious reputation damage, which is hard to recover from.

I've seen automation and visibility tools detect and remediate these types of threats proactively and often in near real-time. By reinforcing and modernizing the security operations center (SOC) to automatically deal with many of these types of threats, organizations can free analyst teams to focus on emerging, novel threats (rather than spending time on mundane or routine investigations).

We're due for a return to the fundamentals of cybersecurity. With so much at stake, I think it's now more important than ever for financial services institutions to protect their systems and data from the core cyberattacks that pose a threat to their customers, the banks and overall reputation.

Based on the work of Splunk's Threat Research Team, here are the four top threats that I believe financial services leaders should prioritize now to make their businesses more secure.

- Matt Swann
Strategic Advisor, Splunk

Threat 1

Account takeovers

The rise of online self-service tools has put a lot of power into customers' fingertips. An enormous volume of our transactions — financial and otherwise — take place online.

From online banking to alternative payment and remittance platforms – even many messaging platforms and super apps – now have a payment component. And they all have one thing in common: an account. For every new account, there's a new opportunity for an account takeover. Any login-based system is susceptible to an attack.

And unlike stealing a single bank account or credit card number, an account takeover can reveal a whole lot more about its target. It gives the attacker access to every aspect of a user account, along with all of the account's capabilities.

On an individual level, 22% of U.S. adults have been subject to an account takeover, totaling roughly 24 million households. The reality is that customers experiencing such financial losses can face even greater emotional impact.

Customers assume that their banks have the right protections in place. So, when someone realizes a large sum of money has disappeared from their account, it can lead to enormous mistrust of the institution responsible for the breach.

What you need to know

Account takeover is considered one of the more harmful ways to access a user's account. According to a recent survey, 32% of account takeover attacks were committed against online banking accounts.

In an account takeover, the attacker typically poses as a genuine customer, user or employee, eventually gaining entry to the accounts of the individual they're impersonating. Rather than stealing the card or credentials outright, account takeover is more surreptitious, allowing the attacker to get as much use out of the stolen card as possible before being flagged for suspicious activity. Banks, major marketplaces and financial services like PayPal are common targets, and any website that requires a login is susceptible to this attack.

For financial services organizations, increasing their account security to include multifactor authentication (MFA) is crucial to protecting private data. Often, attempts go undetected by organizations that lack sufficient identity and access management frameworks to help separate true users from bad actors.

Account takeovers aren't just a consumer concern. Security around supply chains and vendors is particularly susceptible to account takeover attacks, with more than one-third of financial services institutions lacking proper remote access management with MFA.

To avoid illegitimate authentication on cloud applications, no user or device — whether internal or external to the organization — should be implicitly trusted, and access to all resources should be explicitly and continuously authenticated and authorized.

How the attack happens

Some of the most common methods include proxy-based "checker" one-click apps, brute force botnet attacks, phishing and malware. Other methods include dumpster diving to find personal information in discarded mail and outright buying lists of "fullz," a slang term for full packages of identifying information sold on the black market. Once the profile of the victim is purchased or built, an identity thief can use the information to defeat a knowledge-based authentication system.

The threat or attacker can also easily penetrate the network or breach the perimeter when an identity access management framework (IAMF) is weak or non-existent, and when an organization still relies on network or endpoint security. In both instances, because the identity access controls are so lax, the attacker can easily log in with the stolen credentials without being detected — ultimately giving them free rein.

For cybercriminals, acquiring account credentials and personal information (like social security numbers, home addresses, phone numbers, credit card numbers and other financial information) is a lucrative business — whether they choose to sell the acquired information or use it for their own gain.

Between the growing number of phishing attacks, increasing number of user identities and the continued growth of cloud adoption, this type of attack can come from anywhere, including third-party vendors, employees, remote workers and contractors.

Threat 2

Business email compromise

As a result of the COVID-19 pandemic, business invoice scammers took to a new and rapidly growing platform to carry out their attacks: virtual meeting invites.

The FBI IC3 has **received an increasing number of business email compromise complaints** centered on the prevalence of fraud committed through virtual meeting platforms. Through these invites, scammers instruct victims to send unauthorized transfers of funds to fraudulent accounts.

These scammers seek large sums of money and, to make their attack seem more believable, they may impersonate a trusted institution that their marks would not think twice about paying.

What you need to know

Business email compromise attempts to trick victims into paying out a fraudulent (yet convincing) bill addressed to what appears to be a legitimate organization. In reality, the funds go to imposters mimicking suppliers, coworkers or business partners. Often going beyond ordinary fraud, attackers can target banks in emerging markets with limited cybersecurity infrastructure or operational controls, or lure high-profile targets with sophisticated and believable phishing scams.

These cybercrime syndicates are after one thing: money. And lots of it.

How the attack happens

In one attack scenario, cybercriminals use sophisticated malware to bypass local security systems. From there, they gain access to a messaging network and send fraudulent messages to initiate cash transfers from accounts at larger banks. In another instance, the bad actors use targeted spear phishing campaigns to convince stakeholders to transfer large sums of money to their coffers.

Often, hackers will pick targets based on the size of their businesses, location, or suppliers used, and create phony invoices that appear legitimate. With the hope that the victim's accounts payable department is backlogged, they send false invoices with high demands.

A note of caution — high-value wire attacks at institutions with more robust systems likely involve the use of insiders to gain access to systems.

Threat 3

Insider threats

This time, it's personal. An insider threat places the bad actor inside the organization itself, and there's usually a motive behind the attack, such as revenge or greed. Or, in some cases, the insider simply lacks motivation to shore up security weak points, with unintentional threats also making up a percentage of insider threats. With an increase of over 47% in 2022, the prevalence and persistence of insider threats are on the rise, with each incident costing approximately $15M.

Hiring challenges have added a layer of complexity to this threat landscape, with employee turnover in banks reaching an all-time high in 2022. Disgruntled employees on the way out and new hires with red flags on their background checks pose a threat to financial services institutions trying to keep their systems safe.

No matter the reason behind the attack, insider threats have one thing in common: they seem legit. The attacker usually has some degree of authorized access to the systems under threat, making it hard to identify against normal login and usage. This could be a current or former employee, contractor, third-party vendor, remote worker or a cyberspy impersonating any of the above.

What you need to know

The end goal of an insider threat varies, and it can range from stealing classified, proprietary or otherwise sensitive information or assets, either for personal gain or to provide information to competitors. Sometimes, sabotage is the end goal, aiming to create system disruptions that lead to a loss of productivity, profitability and a damaged reputation.

For the financial services industry, insider attacks can range from stealing customers' banking data and money to critically damaging the organization's infrastructure, leading to further financial losses and downtimes for the institution and its customers. One well-known example features a single bad actor that hacked her employer and numerous other companies, taking thousands of social security numbers, insurance numbers, bank account numbers and other personally identifiable information (PII) from customers.

Some institutions are working to combat insider threats by instituting "block leave," or a week of vacation where the employee must disconnect completely from their offices and electronic devices. This gives the company uninterrupted time to access and comb through employees with trading responsibilities' book of business to discover — and discourage — rogue trading practices and fraudulent trades.

How the attack happens

In the case of a malicious insider, the attacker has a distinct advantage in that they already have authorized access to the company's network, information and assets. They may have accounts that give them access to critical systems or data, making it easy for them to locate it, circumvent security controls and send it outside of the organization.

As for an unintentional insider threat, this could be an example of an employee falling victim to another form of cybersecurity threat, such as a phishing scheme or account takeover, and their negligence could be key in letting an attacker abuse the unintentional insider's access.

Whether it's a lone actor working in or adjacent to its victim, a crime ring or hostile nation-state targeting an institution, or a competitor with a vested interest in harming the company, insider threats can do massive damage that might start out looking like normal account access.

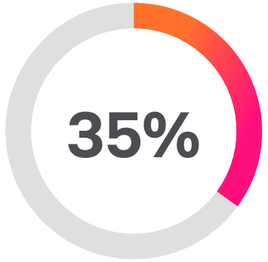
Threat 4

Social engineering attacks

Overall, social engineering attacks cover a range of cyber threats with many sources and motivations, but with one thing in common: they come from human error.

Rather than relying on vulnerabilities in software and operating systems, mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

In the financial services industry, social engineering attacks can affect consumer accounts and the institutions themselves, using threat vehicles like check fraud to exploit security vulnerabilities. When one bank took 50 to 60 days to detect fraudulent checks, it later reported $153M in check fraud losses.



In the financial sector, 35% of businesses consider phishing and malware the biggest cyber risks.

What you need to know

If you want to find an opportunity for a social engineering attack, look at any point of human interaction. The attacks are quite scalable and can be quite simple or very sophisticated. Phishing and malware remain top of mind, with a report of 35% of businesses in the financial sector considering these threats the biggest cyber risks to their business model.

While cybersecurity systems that flag suspicious behavior can prevent the more common, redundant attacks, more elaborate schemes require an “always on” approach to digital resiliency.

Some countries are taking consumer protections to the next level, making financial services organizations responsible for consumer losses, even if the customer initiated the automatic push payment. The time is now for companies to take aim at social engineering threats, even if they do not feel directly responsible.

How the attack happens

Social engineering can take many forms and come from many sources and motivations. Most commonly, it comes in the form of phishing schemes, such as emails that request a customer’s bank account credentials. These phishing emails mimic the financial institution’s typical communications as best as possible, making them hard to detect. Taking it to another level, website spoofing can make a malicious link look like the institution’s webpage, making it even harder for a customer to see beyond the scheme.

Building digital resilience in financial services.

Cyberattacks are inevitable in financial services. But getting back to basics can help financial services organizations focus on the threats that matter most.

With Splunk, financial services organizations can take a proactive approach to security and keep complex systems up and running. Our unified platform helps detect, prevent and respond to all issues, making systems safer and more digitally resilient.

No matter where you are on your path to better resilience, Splunk has the tools to help increase enterprise security and observability using our resilience maturity model:

Splunk helps financial services organizations take advantage of new opportunities:

Prevent major issues

With so much money on the line, the stakes are high in financial services. Organizations can't afford to be reactive. With Splunk, organizations can enhance their security operations center (SOC), improve observability, proactively address more threats faster and use near real-time analytics to fight financial crime.

Remediate faster

Every second a financial services system is down costs the institution huge amounts of money. With Splunk, organizations can speed up investigations and automate up to 95% of incident responses — increasing team efficiency and creating a safe, convenient customer experience.

Adapt to new opportunities

Whether by deconstructing complexity and outdated ways of dealing with issues, or by integrating development, operations and security data in a purpose-built Fusion Center, Splunk helps organizations deliver innovative experiences that meet enhanced customer expectations.

Discover how Splunk can help your financial services institution gain comprehensive visibility across digital systems to respond faster to evolving security threats, keep operations up and running, and unlock future-ready resilience.

Learn more

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.

24.ebook.financial services top 4 cybersecurity threats.r3

www.splunk.com/FSI

splunk>