FORTRA™

The Financial Industry Threat Landscape:

Top Threats and Proactive Security Best Practices

Money may or may not be the root of all evil, but it certainly seems to be the root of nearly all cyberattacks.

This past year, 95% of attacks were financially motivated, according to the Verizon 2023 Data Breach Investigations Report (DBIR). It's clear that any company that manages money – and especially those that are in charge of a lot of it – has a huge, dollar-sign target on their backs. Since threat actors aren't likely to back down, it becomes the duty of security practitioners to step up.

The first step in that process is being painfully aware of our surroundings. Let's take the cover off the motivations, methods, and malpractices of cybercriminals targeting the financial services sector and familiarize ourselves with the best proactive ways to stop them.

Holes in the Security Fabric of Financial Services

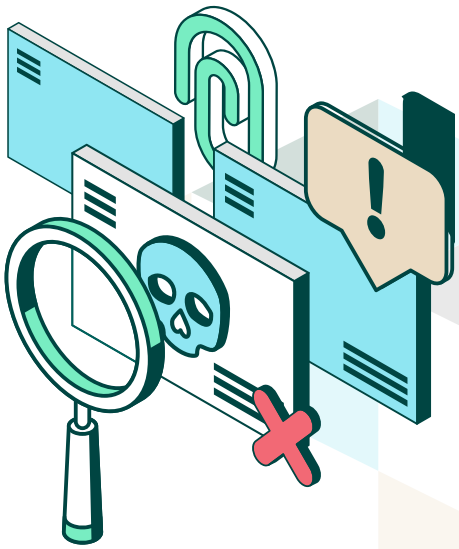
Verizon's DBIR found a total of 2,527 cybersecurity incidents in the financial sector in 2022. 690 of these incidents had confirmed data disclosure. More proactive preparation could have led to more positive outcomes for the financial services sector, as indicated by breaches such as these:

- Last year, a Square (now Block) employee illicitly downloaded the records of approximately 8.2 million current and former customers. Without even advanced exploitative strategies – the unwitting inside actor breached these records "while managing processes included in their day-to-day tasks" - millions of names, brokerage account numbers, portfolio holdings, and stock values were revealed.
- In 2019, First American Financial Corporation suffered from a Business Logic Flaw, in which sensitive information wasn't protected by even the simplest of authentication requirements. This resulted in stolen customer names and email addresses, along with the phone numbers of closing agents and buyers.
- External threat actors accessed Flagstar Bank in 2021 (the incident was reported in June of 2022) and accessed the sensitive information of nearly 1.5 million people. One of the largest banks in the U.S., Flagstar assets total over $30 billion dollars. To remediate the situation, the bank ended up paying for two years' worth of identity theft monitoring and protection services for all (1.5 million) impacted individuals.

The finance industry pays out the second highest amount for its data breaches compared with any other industry. At an average of $5.9 million per confirmed case, breaches are costing finance firms 28% more than the global average. The top attack vectors are phishing and stolen credentials, respectively, and each breach could give criminals access to millions of client and transaction records. It's a high-stakes environment, and the unilaterally high breach rates show that threat actors are benefitting from circumstances that put them at low risk, with sky high rewards.

The global cybersecurity in financial services industry is "poised for robust growth" and is expected to reach nearly 43 billion in global revenue this year and boasting a 9.81% compound growth annual rate (CAGR). However, it's clear there is a disconnect between these record high breach rates and the amount of cybersecurity investment within the industry. Both are high, and that is where the discrepancy lies.

While protections, strategies, stacks, and technologies are all central to staving off attacks, so is the experience required to use them, and to use them well. Proactive, or offensive, security practices put teams, tools, and talent to the test to see if all these cybersecurity investments are really paying off – or if they perform better on paper than in the real world.



Why Proactive Security is Beneficial for the Financial Sector

In short, proactive security practices are ways a company can assess their environments for security weaknesses before an outside attacker hacks them.

When practices like pen testing and red teaming are implemented, the organization can get an idea of what an attack would look like and walks away the wiser for it. They have time to rehash what went wrong, deploy additional training, close security gaps, implement new processes, and ultimately live to defend another day.

Without it, the company is potentially caught completely off guard and their only real-world training for such a high-stress situation is an attack. As the adage goes, when the time for action is here, the time for preparation is past.

So goes cybersecurity, and this has been the problem among underprepared organizations from the beginning. Meeting a cyberattack head-on is so much more than deploying the right security solutions and having them all check out on paper. It is battle-testing those defenses and vetting for vulnerabilities. It is making sure that even if those vulnerabilities are patched, the network can't be exploited in any other way. And it is making sure that when the time comes, your team is ready.

A genuine cybersecurity incident can mean 24 hours or more of analysis, defense, and threat mitigation. It may require needing to find a needle in a cloud-based haystack when your network isn't fully mapped. Difficult decisions up and down the chain of command will be required, and teams will need work long hours all while sustaining laser-like focus in supremely stressful environments. Does your team know the drills?

After rounds of continuous proactive security training, they will.

Top Threats

So, what will SOCs be defending against? It is important to find out. After all, an ounce of prevention is worth a pound of cure.

Knowing the tactics is tantamount to getting your marching orders for the security battle ahead. In that spirit, here are some of the top avenues exploited by cybercriminals to cause havoc in the financial services sector today.

- **Third-Party Risks |** Many FinTech companies rely on third-party vendors for services like payment processing or data storage. These vendors may have cybersecurity weaknesses of their own, which can spread to the company's data and systems. Finance firms must conduct thorough due diligence on third-party vendors *before* signing the contract to ensure adequate security measures are in place. The approval process should include vetting for supply chain threats.
- **Insider Attacks |** Within the finance sector particularly, insiders can represent an extraordinarily high risk. In South Africa, a PostBank employee compromised sensitive customer bank data by copying a master key. The incident cost PostBank a total of $58 million. However, unintentional insider threats may be an even more prominent concern. According to a recent Ponemon Institute Report, negligent insiders drive 56% of all insider incidents and cost an average of $484,931 each time. This is due largely to weak passwords, incorrectly escalated privilege, successful phishing attempts, and other poor security practices such as misplacing documents, sending files insecurely, or accidentally inputting the wrong sender address in an email. Whether malicious or negligent, the bottom-line is the same. As financial institutions become more decentralized and increasingly digitized, the potential for widespread, employee-spurred harm only gets worse.
- **Ransomware |** The median cost of ransomware has doubled in just the past year, according to the Verizon 2023 Data Breach Investigations Report. Global financial services institutions have shelled out over $32 billion in total ransomware costs over the past five years, a Comparitech report states. With payouts this high and money motivating 95% of all data breaches, it would be safe to say that ransomware will continue to be a popular weapon of choice against financial institutions.
- **Business Email Compromise (BEC) |** While ransomware might be costly, BEC is even more so. According to the FBI 2022 Internet Crime Report, ransomware-related losses totaled an impressive $34.3 million last year, but BEC-related costs trumped them at a massive $2.7 billion – dwarfing them 78 times over. These schemes are only made more effective by Artificial Intelligence, with attackers cloning the voice of a supply chain partner or crafting a highly personalized email to get you to wire money to the wrong party.
- **Basic Web Application Attacks |** Nearly eight in ten (77%) of all data breaches within the sector are attributable to the simplest of cybersecurity hacks. Unfortunately, the vast majority of fiduciary organizations fall prey to low-level attacks. These include SQL injections, fuzzing, cross-site scripting, credential stuffing, and other non-sophisticated techniques. This year alone, basic web application attacks, miscellaneous errors, and system intrusion accounted for 77% of all breaches in the finance and insurance sector.
- **Data Aggregation Dangers |** Financial data aggregation is a boon to the industry, and customers appreciate being able to see all their bank accounts at a glance. But is the reward worth the risk? Customers can easily expose their information due to credential stuffing, API-based attacks, and password pilfering. All of this results in unauthorized transactions, identity theft, and stolen data. Additionally, many aggregators may not be under the same regulatory oversight as financial firms, especially when it comes to privacy. When partnering with a data aggregation company, make sure they understand the risks involved and are well suited to deal with them. If they're not, you have to be.
- **Blockchain and Cryptocurrency |** The ENISA Threat Landscape 2022 Report notes that 83% of respondents are concerned with the security of cryptocurrency exchanges. And they have good reason to be. As other exploits ease off the gas, ransomware is gearing up to have its second-biggest year ever in crypto-related crime. Ransomware infiltrates via phishing, among other routes, and the internet abounds with bitcoin-based dupes. Additionally, API keys can be stolen from trading platforms and reprogrammed to withdraw funds, and cryptocurrency registration forms are still subject to SQL injection and other basic web application attacks.

There is no shortage of attack vectors in the financial services industry, and each day threat actors are sharpening their attacks. While it is good to be aware of the threats today, proactive security measures that are constantly updated with the latest techniques are critical to staying ahead of attacks tomorrow.

A Heavily Regulated Sector: Protecting Precious Data

It's no wonder that the regulatory commissions that oversee the industry have intense data privacy requirements. They include:

- PCI DSS | This standard regulation is intended for organizations that transmit, store, or process payment card information, including those that create the software to do so.
- SOX, SOX 404 | The Sarbanes-Oxley Act requires accountable financial record keeping from publicly traded U.S. corporations.
- GLBA | The Gramm-Leach-Bliley Act requires financial institutions to be transparent about their data sharing practices and safeguard sensitive information.
- GDPR | This wide-ranging privacy regulation applies to how business, including financial services organizations, handle the sensitive, personal data of those within the European Union.
- BSA | The Bank Secrecy Act is a series of laws aimed at combating money laundering and the financing of terrorism.
- PSD 2 | The Payment Services Directive is another EU legislation that enforces stronger security for customer payment services, particularly authentication and third-party access to customer accounts.
- FINRA (SEC's Regulation S-P) | This nongovernmental regulatory organization requires the U.S. broker-dealer industry to have written policies and procedures designed to secure customer data.
- FFIEC Standards | The Federal Financial Institutions Examination Council has a diagnostic test that helps financial services institutions identify their level of risk and determine the maturity of their cybersecurity defenses.
- FTC Safeguards | This recently revised ruling of the U.S. Federal Trade Commission (FTC) requires all non-banking financial entities to maintain comprehensive cybersecurity protections to secure customer financial data.

Designed to protect companies as well as consumers, these guidelines carry heavy penalties and fines if not kept.

Foundational Security Principles

Before proactive security can take place, financial services organizations need to make sure foundational security principles are at the heart of their strategy. Then, offensive security measures will have something worth testing.

Securing Sensitive Data

If financial data is what cybercriminals want, then it's what defenders must protect the most. Managed File Transfer (MFT) encrypts and automates the file transfer process, making the movement of information efficient, reliable, and safe. This is key for avoiding anything from mis-sends that land emails in the wrong hands, to man-in-the-middle attacks that can steal or manipulate data in transit.

Protecting sensitive financial data also comes down to good identity and access management (IAM). The right IAM platform gives you not only the data, but the context you need to make a quick decision. IAM systems account for password management, policy management, provisioning, access governance, and what can be complex identity repositories.

Keeping Ahead of Attackers

A crucial element of cybersecurity today, especially when dealing with an industry as inundated with attackers as financial services, is responding at scale. Robotic Process Automation (RPA) can automate key security functionalities within the financial services sector, allowing FinServ SOCs to stay ahead where they might otherwise fall behind. Offloaded tasks include secure file transfers, service desk requests, credit card application processing, and new account data entry, to name four.

Proactive Security Best Practices

There are countless ways in which financial institutions can order their security stack and arrange their strategy, but once the basic principles are in place, it is time to test defenses.

This is where proactive security measures come in.

Vulnerability Management

This cannot be left off the table for highly regulated industries like finance. A good vulnerability management solution should be a fixed part of the security routine: the network should be regularly scanned for any unpatched vulnerabilities, and patches should be applied.

Since there are always updates, rollouts, and new applications hitting the environment, security assessments should be done on a regular basis. Today, vulnerability management needs to work just as well in the cloud as it does on-premises (although it should work well there, too) and SaaS solutions make performing these checks with regularity even more resource-efficient. You may also want to look for dynamic web application testing to gain insight into the security state of your organization's web applications, like the digital banking apps we've come to rely on.

Another key element of vulnerability management, and one that often gets overlooked, is knowing how you rank compared to the other companies threat actors are looking to victimize. While comparing ourselves is usually counterproductive, in some cases it can be beneficial. Specifically, look for a solution that can tell you how you stack up against your industry peers when it comes to threat prevention techniques. For example, what is the average time it takes you to fix vulnerabilities? What should it be? This is a good litmus test to see if this is an area your organization needs to prioritize, or if you're running with the pack. Remember, attackers pick off the ones that fall behind.

Penetration Testing

Once the vulnerabilities have been discovered, it's time to see which ones can cause the most potential harm to the enterprise. Penetration testing determines whether the identified risks pose a real threat to data, and if so, which should be prioritized. Key features to look for in a penetration testing solution include:

- **Multi-vector testing capabilities |** Can you test not just your network infrastructure, but other endpoints like web applications to reveal exploited vulnerabilities?
- **Strategic automation |** Optimize the process by automating the time-consuming and repetitive aspects of pen testing.
- **Certified exploits |** Get professionally written and validated exploits that are constantly updated to test your systems for the real-world.
- **Extensive, customizable reporting |** Validate compliance with industry regulations with comprehensive reporting capabilities post-test.

The right solution will provide centralization to gather information, exploit systems, and generate reports all in one place to make your testing standardized and efficient.

Red Teaming

Red team engagements are as close to a real-world attack scenario as you're going to get without risking data loss. These all-out engagements have red teams engage in actual tactics a cybercriminal could use in order to test your organization's response capabilities, using best-in-class red teaming solutions to mimic the techniques of a long-embedded actor. Financial services firms can go a step further by also investing in advanced toolsets that bring red team operations to a whole new level. With these solutions, your SOC trains against ever-advancing adversarial techniques that target each segment of the attack kill chain, making sure they're ready end-to-end.

Stay Safe Out There

We all know that dealing with the consequences of financial data loss is not cheap. Cyberattacks cost the banking industry $18.3 million annually per company, and every year attackers are out for more and more money. As noted in the recent Verizon DBIR, 85% of data breaches were financially motivated in 2021 and last year the number jumped up to 90%. By the time the report came out this year, a whopping 95% of data-targeted attacks were spurred by economic drivers.

Which means that so long as the financial services sector continues to exist, there is always going to be the need to stay battle-tested and attack ready.

Financial services organizations can leave nothing to chance when it comes to securing their digital enterprise. In response to tougher-than-every cyberthreats, the solutions on the market today are some of the best the industry has ever seen. Fortra can help you dive into proactive security habits and prepare your SOC for what's next. Because as long as money is still the number one attack motivator, no commercial organization is safe.

However, by continuously subjecting teams and technologies to the latest techniques, organizations can increase the likelihood that the next organization to be breached won't be theirs.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-gd-1023-r1-vm