HADRIAN

WHITEPAPER

The financial sector against today's tough cybersecurity risks

Table of Contents

Manage Your Company's Threat Exposure

CISOs and security managers within the financial sector are up against a tough battle when it comes to hackers. That's because the financial sector is a target-rich environment for sophisticated cybersecurity threat actors. It's no wonder that breaches, and threats of breaches, are increasing exponentially each year within this sector.

The financial sector is particularly vulnerable due to its vast amounts of sensitive information on its clients, and its extensive use of third-party services. These third-party services create an expanded attack surface, and thus a greater number of entry points for hackers. CISOs at financial institutions need to be extra vigilant of these extended attack surfaces created by third-party vendors. It's all too easy to be unaware of an unsecured S3 bucket in AWS, for example, created by a developer of a third-party service.

Other examples of today's third-party risks financial institutions could face include:

- Legitimate third-party software or infrastructure that are misconfigured, such as HR tools;
- Legitimate third-party software that has vulnerabilities, such as publicly known CVEs, and in some rare cases, like with SolarWinds--where development of has been compromised and vulnerabilities deliberately inserted;
- Illegitimate third-party software or infrastructure, or shadow IT, acquired at an organization without being first approved by the IT or security team to ensure it complies with regulations/security standards;
- In-house applications built using open-source software that in very rare cases could have been maliciously compromised, or more likely, wasn't built properly in the first place.

However, third-party vendors aren't the only weak spot in a financial institution's attack surface. According to a recent McKinsey survey,[1] financial services companies have more recently evolved into technology-driven companies—heavily investing in DevOps (software development and IT operations), machine learning and AI, and cloud and edge computing, to name a few.

This increased use in technology naturally increases the potential risk of breaches.

"As financial-services companies around the world race to keep pace with a rapidly evolving technology landscape, they should consider not only what benefits new emerging technologies offer but also what risks they introduce," McKinsey says.[2]

McKinsey's survey shows that financial institutions are currently falling short of addressing these added security risks. Most survey respondents said they need to strengthen critical cybersecurity capabilities, including third-party or supply chain management and privileged access management (PAM).

> **"As risks mount, now is the time to future-proof your environment."**
>
> McKinsey

Cybersecurity Trends Impacting Finance

Supply chain attacks increased by 742% between 2019 and 2022.[3] Developers like to use open-source code or third-party APIs components to help speed their development times, but there is always the chance that these codes or components could be compromised.

Software is built out of hundreds or sometimes even thousands of components, and chances of vulnerabilities increase with each component added. The more components, the greater the risk. Threat actors can inject malicious code easily into the software build environment.

Gartner predicts that by 2025 about 45% of organizations will have experienced attacks on their software supply chains.[4]

SecurityWeek names these current threat trends for supply chain cybersecurity:

A State-sponsored attacks that look to destabilize economies

B Concentration risks within extended supply chains, including reliance on a single supplier or fourth parties

C Sophisticated supply chain attacks that leverage AI/ML

D Joint ventures among technically skilled criminal groups to target supply chains

E Open-source software (OSS) corruption with malicious packages on public repositories.[5]

Other experts cite these key cyber vulnerabilities for the finance sector:

F **Multi-package attacks**
Attackers split malicious actions across multiple packages to evade detection.

G **Fraudulent sources**
Cybercriminals impersonate legitimate and well-known sources while introducing malicious code.

H **Use of abandoned digital assets**
Attackers exploit old assets, like deserted AWS buckets, to introduce malicious code and make them seem like a trusted delivery mechanism.

I **Social engineering**
Social media is used to establish trust in fake developers promoting malicious open-source packages.[6]

Questions for CISOs at Financial Institutions

Managing the attack surface in the financial sector is challenging. Financial institutions need to find clear best practices to assess and monitor their attack surface, while ensuring they meet important regulations with limited resources.

According to McKinsey, when financial institutions pursue new technology, they should lay the foundation for good cybersecurity by asking themselves these four questions:

01 Do our technology priorities align with our security capabilities?

02 Are we investing in the right technologies and cybersecurity capabilities?

03 Do we have the right metrics and reporting to identify cybersecurity strengths and weaknesses?

04 Do we have the right talent to close cybersecurity gaps now, and into the future?[7]

How to Align with the Best Cybersecurity

The best defense is a good offense. Offensive cybersecurity policies and practices assess the infrastructure through the eyes of a threat actor. Instead of focusing on merely defending the perimeter in a reactive way, it focuses on the realistic current ways hackers attack. That way, organizations can proactively mitigate threats before they are exploited. Offensive cybersecurity works on identifying gaps in cybersecurity rather than mitigating the effects of an exploit.

Based on the attack patterns that we have seen, Hadrian estimates that attacks on software supply chains are set to rise. (Why attack a single target when dozens or even hundreds of targets can be attacked simultaneously?) But these are only part of a larger picture.

The current threat landscape is evolving rapidly, prompting a need for new and better cybersecurity strategies. Expanding and increasingly complex attack surfaces provide more opportunities for threat actors to exploit. Additionally, the rise of mass attacks, as opposed to targeted high-return ones, is creating further challenges for cybersecurity teams. Traditional defense methods are no longer suitable. It's time to go on the offense.

Checklist for Comprehensive Cyber-Defense

Monitor external-facing assets to find weaknesses before exploited.

Hadrian's AI Orchestrator is capable of quickly identifying complex attack paths and vulnerabilities that may be unknown to security teams. We do this by leveraging a combination of passive data sources, active scanning, and machine learning models.

Defeat attacks targeting your software supply chain.

Hadrian continuously assesses third-party applications for risks that could result in a breach. Our in-house hacker team constantly develops detection modules to identify new software supply chain threats. Our platform verifies when your risks are exploitable and shares the most effective remediation steps with you.

Uncover all third-party applications.

Hadrian's probes can identify over 10,000 SaaS applications and 1,000s of software packages and versions, to find every application. We continuously scan the internet to discover your assets. Our probes inspect technology, versions and configurations, to identify potential threats to your security.

Find forgotten applications.

When third-party software vulnerabilities are discovered, without an updated and accurate inventory list organizations struggle to confirm whether they are deployed in their environment. We find and verify your abandoned digital assets, including deserted AWS buckets. Attackers use these to introduce malicious code by making them seem like a trusted delivery mechanism.

Respond to zero days.

New zero days are often specific to certain vulnerable software versions or configurations. Minimizing the time spent verifying the software deployed is critical to preventing attacks. Our in-house hacker team constantly adds new detection modules to identify any emerging threats. We identify zero-day threats and immediately prioritizes them for remediation.

Verify remediation.

Organizations must ensure that risks to their third-party applications have been successfully completed. Overlooking an application or a threat could lead to a breach. Our regression testing automatically verifies that your remediation activities have successfully resolved risks and alerts you if you've failed to do so.

Verify your posture.

Hadrian reveals the posture of your organization and the impact of a third-party software compromise. Reassessing risks enables your security team to confirm that threats are no longer present so you move on to the next task. As you remediate the risks, Hadrian dynamically updates the security level score of the organization.

Scan for threats continuously.

We provide real-time discovery of new and changing third-party applications in your attack surface to identify potential threats and give you complete visibility of your entire attack surface.

Remove false positives.

Hadrian's Orchestrator AI verifies whether weaknesses could be exploited by an attacker by testing with initial access can be achieved, removing false positives.

Employ risk-based prioritization.

Hadrian integrates asset context and threat intelligence to prioritize risks based on potential impact, promoting the efficiency and effectiveness of your workflow. We provide centralized asset management and assign them to your users.

Secure your software development lifecycle (SDLC).

By conducting penetration testing on new code in production, Hadrian secures your SDLC. At Hadrian, we believe Automated PenTesting is the only way to eliminate software bugs in a world that demands an increasingly rapid development cycle. The pace of modern software development leaves little time to manually assess risks.

Sources

01 The cyber clock is ticking: Derisking emerging technologies in financial services, March 11, 2024, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services

02 McKinsey

03 https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security

04 https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

05 SecurityWeek, Supply Chain Cybersecurity Insights, 2024, https://www.securityweek.com/cyber-insights-2024-supply-chain/

06 https://fluidattacks.com/blog/supply-chain-financial-sector/#why-is-the-financial-industry-vulnerable-to-supply-chain-attacks

07 McKinsey