autorabit

EBOOK

Top 5 Threats to Financial Data Security and Compliance in 2025

INTRODUCTION

Finance companies are always near the top of the list of industries most frequently targeted by cybercriminals. This is because of the degree of sensitivity of the information inherent in financial services—such as personal identifiable information (PII), financial data, and investment data.

And when these attacks occur, the damage can be massive. On average, breaches to financial systems cost around $6.08 million.

The financial impact to these organizations is far from the only risk. The customers themselves suffer consequences when their information is exposed. In 2023, fraud cost Americans $10 billion.

Exposures also threaten the financial organization's compliance with data security regulations. The exact regulations that apply to each financial company depend on where it is located, but failing to adhere to regulations, such as the Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), Sarbanes-Oxley Act (SOX), and Payment Card Industry Data Security Standard (PCI DSS), can lead to fines and penalties.

Understanding the risks is the first step toward properly protecting sensitive information. Cybersecurity threats have grown increasingly dangerous and will continue to do so into 2025.

We'll explore these five major threats to financial data in 2025 and what you can do to prepare for them:

01

AI-Driven Attacks →

AI-DRIVEN ATTACKS

Artificial intelligence is entering every aspect of our digital environments. It’s no surprise that cybercriminals are leveraging the power of AI to threaten sensitive data in historically targeted industries like finance. Their ability to threaten protected information will grow alongside their increased maturity.

Cybercriminals will increasingly use AI to automate and scale attacks, personalize phishing attempts, and uncover system vulnerabilities.

Identity verification can also become more difficult in the face of the capabilities of AI tools. Deepfake technology can complicate identify verification and threaten traditionally secure practices.

AI is lauded for its ability to expedite processes like code generation, but this capability is also what makes it so dangerous. These attacks can be executed at a much faster rate than previously thought possible, which makes it much harder for financial systems to guard against them.

How to Prepare

A continuously updated system is best prepared to fend off AI-driven attacks. This means it’s essential to strengthen and streamline your Salesforce DevOps strategy with automated tools such as CI/CD and static code analysis. An optimized application lifecycle is better equipped to produce error-free, secure updates and applications. Frequent security patches and the elimination of bugs in live environments reduce the vulnerabilities that can be exploited by AI threats.

End-point security is important in data security strategies. This includes ensuring all team members connected to your IT network maintain secure practices while also implementing a zero-trust model for permissions. Strong access controls with multi-factor authentication are nonnegotiable.

Behavioral biometrics such as typing speed and unusual activity patterns can be tracked for suspicious activity. Outliers can be flagged for further investigation and can root out AI attacks before they can infiltrate IT environments.

02

Ransomware

RANSOMWARE

Ransomware has seen a huge spike over the past few years and will continue to grow in complexity and financial damage. In fact, the average cost of a ransomware attack jumped more than 500% between 2023 and 2024 to about $2 million.

Attackers are focusing on stealing sensitive data before it can be encrypted and threatening to release it to the public if their demands aren't met. This can lead to protected information ending up on the black market, which is hugely detrimental to customers and creates compliance failures for finance companies.

PII, financial data, and investment information are highly targeted by cybercriminals because they know how harmful it can be when the information is exposed, which makes finance companies prime targets for ransomware.

How to Prepare

Ransomware is effective in two main ways: by threatening to expose sensitive data and threatening to remove access to important information. The second threat can be mitigated with a contemporary data backup and the means of quickly recovering this data. Automated backup snapshots should be scheduled to automatically capture system data multiple times each day.

Segmenting critical systems mitigates the damage should a cybercriminal gain access to your IT environment through ransomware. Limiting the spread will reduce the potential for damage.

Email is a frequent entry point for ransomware. Employ an email security solution that detects and blocks ransomware payloads while also using antivirus and anti-malware scanning for additional layers of protections. Continuously updating permissions ensures each team member is only able to access the data needed to complete their tasks. This further segments your system should a breach occur. An automated security posture management tool can scan for these settings to keep everything in accordance with best practices.

And since these attacks often rely on tricking team members, continuous training on how to spot fraudulent messages is incredibly important.

03

Supply Chain Attacks →

SUPPLY CHAIN ATTACKS

Finance systems encompass a variety of tools to best serve customers. Software, cloud providers, and Internet of Things (IoT) devices are all potentially vulnerable to cybercriminals, which could become costly mistakes.

These supply chains introduce numerous points of connection that all need to be protected vigorously. If not, attackers will exploit these supply chain vulnerabilities to gain access to finance networks.

Indirect attacks are nothing new, but the expansiveness of finance networks expands the risks of connected parties, leading to exposures, corruptions, and breaches of sensitive data. And even if the exposure is the result of a third-party application, the finance company itself ultimately bears the responsibility for the negative results.

How to Prepare

Finance companies should always conduct thorough assessments of third-party vendors prior to implementation. Verify their cybersecurity standards align with your own and ensure their technology seamlessly matches your current IT environment to prevent holes in coverage.

The points of connection can be exploited to grant access to unauthorized users. A zero-trust architecture authenticates and verifies every user and device, regardless of location, before granting access.

Frequent audits of the vendors' cybersecurity controls and compliance with agreed-upon standards should be conducted. This ensures everything is up to date and the established requirements are upheld.

Knowledge is the key to protecting sensitive data. Finance companies need to stay informed about emerging supply chain threats and fortify their systems prior to an attack. An incident response plan should be in place to swiftly respond in the event of a breach. Share this plan with vendors to keep everyone on the same page and ensure a robust response to an attack.

04

Internet of Things (IoT) Vulnerabilities

INTERNET OF THINGS (IOT) VULNERABILITIES

As technology progresses, the number of connected devices within a financial network grows. These devices enable organizations to offer better service to their customers with heightened connectivity and oversight, but they also create data security risks.

Every device connected to your platform is a potential entry point for cybercriminals. And if strict cybersecurity measures aren’t implemented and followed, your likelihood of experiencing a breach increases.

Manipulation of device functions is just one of the ways cybercriminals can wreak havoc on financial systems if you aren’t properly protected.

How to Prepare

An infrastructure of security throughout your IT environment provides the support needed to safely utilize IoT devices. Segmenting networks into isolated zones ensures these devices are separated from critical systems. All devices and users should be authenticated through multiple layers before gaining access to the network. Automated support through Intrusion Detection and Prevention Systems (IDPS) monitors traffic for suspicious activity.

The devices themselves must also be properly configured by disabling default usernames, passwords, and unnecessary features. Proper setup with a zero-trust approach reduces vulnerabilities. Certificates or hardware-based authentication can also be utilized to verify the legitimacy of a device before connecting it to your system. And once these devices are connected, they must remain up to date with security patches and functionality updates.

Regular risk assessments should be conducted, including penetration testing and the ongoing evaluation of the security practices of third-party vendors. Consistent monitoring will alert your team members to any potential vulnerabilities while also empowering them to respond quickly should an intrusion be detected.

05

Data Manipulation

DATA MANIPULATION

Not all cybercrime is aimed at extracting valuable data for financial purposes. Sometimes, the goal is just to upend operations. Data manipulation refers to attackers targeting the integrity of financial data by altering transaction records and investment data.

These types of attacks have the potential to undermine trust in our financial systems. State-sponsored attacks are increasingly common, and eroding trust in our financial systems sows chaos in our society. Corporate espionage and hacktivism are other potential motivations for manipulating financial data.

How to Prepare

A multilayered approach instills protections that safeguard data integrity, identify and mitigate vulnerabilities, and prepare for timely responses should an attack occur.

Encryption is critical for protecting sensitive information. Beyond that, cryptographic hashing creates unique digital fingerprints for data records, so any unauthorized changes can be easily detected. Blockchain technology can be used for unalterable audit trails that make all data changes transparent and traceable.

Automated monitoring and detection tools need to be implemented to expand the reach of your team. AI-driven tools can be leveraged to monitor behavioral analytics for suspicious activity. Combine that with real-time alerts for notification when unauthorized data changes occur.

Secure development practices with the assistance of static code analysis enable your team to produce flawless, reliable coding updates and avoid unnecessary vulnerabilities. Injection attacks are common in applications and updates. Input validation should be leveraged to avoid malicious manipulations of data.

A robust series of audits, backup snapshots, and a continuously updated recovery strategy need to be maintained. Only a comprehensive strategy will offer the protection financial systems need to properly guard data from dangerous tampering.

CONCLUSION

Financial organizations are trusted with their customers' most sensitive information. Failure to properly protect this data can lead to loss of institutional trust, falling out of compliance with data security regulations, and serious financial problems for customers.

A robust and comprehensive data security strategy will provide the level of support needed to remain secure in the face of increased cyberattacks and data security risks. Maintaining automated oversight, ensuring a streamlined recovery strategy, and focusing on an error-free development pipeline will all support remaining secure and compliant.

The use of automated release management tools, static code analysis, and a robust data backup tool are nonnegotiable for protecting financial information. AutoRABIT's comprehensive Salesforce DevSecOps platform provides a holistic approach to data security that helps teams properly protect sensitive data.

Financial organizations serve a very important role in helping people manage their money and prepare for a secure and comfortable future. Failing to protect sensitive data can have dramatic impacts on customers' quality of life. The good news is there are automated tools and intentional practices that will enable financial organizations to maintain strong barriers between protected data and malicious attacks.

ABOUT AUTORABIT

AutoRABIT is a DevSecOps suite for SaaS platforms that automates and accelerates the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. AutoRABIT tools help enterprises achieve higher release velocity and faster time to market.

Features include static code analysis, automated metadata deployment, version control, advanced data loading, orgs, sandbox management, test automation, and reporting. Its services complement and extend Salesforce DX.

AutoRABIT ARM accelerates the delivery of business innovation with automated release management tools, including CI/CD automation, Data Loader Pro, and version control integration.

AutoRABIT Vault is a backup and recovery solution that streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and provides end-point data protection in the cloud.

CodeScan gives Salesforce developers and administrators full visibility into code health from the first line written through final deployment into production, along with automated checks of Salesforce policies.

Visit us at www.autorabit.com to learn more.

CERTIFIED
+ COMPLIANT

SOC 2 TYPE II CERTIFIED

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

ISO 27001 INFORMATION SECURITY CERTIFIED

HIPAA COMPLIANT