2025 State of Financial Services: Hidden Dangers in the Vendor Ecosystem

For the best experience, view the interactive report: content.blackkite.com/ebook/financial-services-tprm-report-2025/

Introduction

The greatest threat to your financial organization isn't coming through the front door.

The financial services sector is widely protected by stringent regulations, government takedowns of the bad actors who target them, and robust defenses against direct cyberattacks and breaches.

- These companies generally have Chief Information and Security Officers in place keeping a watchful eye on their systems and processes.
- The largest ransomware groups that favored financial services organizations in their attack campaigns have been dismantled by government agencies.
- And we have seen a dramatic decrease in ransomware attacks on financial companies as a result over the last two years.

But this perceived safety creates a dangerous blind spot. The true, and often overlooked, vulnerability lies within the extensive network of third-party vendors that serve the financial services sector.

We analyzed a sample set of vendors with 10% or more clients in the finance industry (amounting to 140 vendor companies). Among these vendors, a multitude of weaknesses exist that pose a considerable risk to financial institutions, potentially impacting their operations and security. While banks and financial institutions themselves may possess strong defenses, the companies providing services to them often lack the same level of security. If these vendors are compromised, attackers can gain indirect access to the financial institutions they serve.

This report explores the shifting landscape of cyber threats in the financial sector, highlighting the critical importance of understanding and mitigating the hidden dangers within the vendor ecosystem.

Key Takeaways

Declining Direct Ransomware Attacks

Direct ransomware attacks on the financial sector have decreased significantly due to strong defenses and the disruption of major threat groups.

Shifting Attack Focus

Attackers are increasingly exploiting weaker links within the financial ecosystem, primarily through third-party vendors.

Pervasive Vendor Vulnerabilities

A significant number of vendors serving the financial sector exhibit critical security weaknesses, including outdated systems, poor patch management, and credential exposures.

Supply Chain Impact

Vulnerabilities in vendors can lead to direct security risks for financial companies relying on them, even from non-cyber events like service outages.

False Sense of Security

Financial institutions may have a false sense of security due to their own robust defenses, overlooking the substantial risk posed by their supply chain.

TABLE OF CONTENTS

01 | RANSOMWARE TRENDS
How financial organizations fare against ransomware attacks.

02 | VENDOR TRENDS
Risks lurking in the financial sector's vendor ecosystem.

03 | SUPPLY CHAIN IMPACT
Real-world cascading effects of vendor incidents in financial ecosystems.

04 | NEXT STEPS
How to protect your organization from third-party breaches.

05 | METHODOLOGY
Learn about the methodology behind our primary research.

Start with an understanding of ransomware in finance.

NEXT PAGE

Ransomware Attack Trends in the Financial Sector

Where the Real Risk Lies

Ransomware Attacks on Finance Trend Downward

In 2023, 191 companies from the financial sector were targeted by ransomware attacks. This number dropped to 156 in 2024. As of mid-2025, only 55 incidents have been recorded.

Ransomware Attacks on the Financial Sector

191	156	55
2023	2024	2025 (June)

So, what explains this notable decrease? We'll get to that soon. But first, let's look closer at the ransomware activity within the industry.

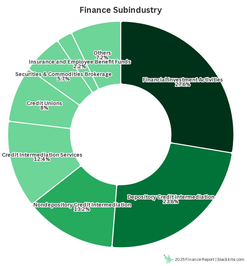
Subindustry Review

The financial sector is not a monolith. Ransomware actors tend to focus on specific subindustries with varying frequency.

- Financial Investment Activities accounted for the highest share of attacks at 27.6%, likely due to the direct access to funds and sensitive customer data.
- Depository Credit Intermediation (e.g., traditional banking institutions) followed closely at 23.6%, showing that wealth management and private equity are also high-value targets.
- Interestingly, Nondepository Credit Intermediation (such as leasing and lending companies) represented 13.2% of cases, slightly ahead of Credit Intermediation Services at 12.4%.

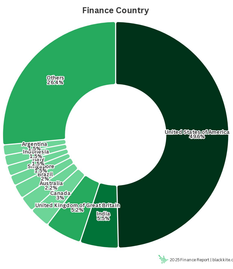
These figures suggest that attackers are diversifying their targets within the sector, although traditional banks still bear the brunt of activity.

Ransomware Attacks by Finance Subindustry



2025 Finance Report | blackfrio.com

Ransomware Attacks on the Finance Sector by Country



2025 Finance Report | blackfrio.com

Country Review

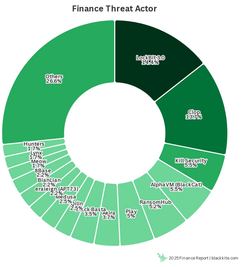
The country distribution shows that the biggest targets are among the richest for big payouts.

- The United States remains by far the most targeted country in financial ransomware cases, accounting for 49.6% of all incidents. This dominance is expected, given the concentration of financial infrastructure, fintech innovation, and capital in the U.S. market.
- Following the U.S., countries like India (5.5%), the United Kingdom (5.2%), and Canada (3%) also emerged as notable targets. The relatively high number of attacks in these regions reflects both their digital maturity and the attractiveness of their financial ecosystems.
- The "Others" category still makes up 26.4%, which hints at the growing global spread of ransomware beyond traditionally targeted geographies.

Threat Actor Review

The threat actor distribution shows that while the big names still matter, fragmentation is real.

- LockBit 3.0 and Clop led the chart with 14.4% and 13.7% shares respectively, both known for bold, large-scale operations.
- AlphaVM (BlackCat), KillSecurity, and RansomHub made up the mid-tier group with around 5–5.5% each.
- What's most striking is the 26.6% share attributed to "Others", which includes numerous emerging or short-lived groups. This reinforces the idea that while the dismantling of major groups may have reduced direct threats temporarily, the ransomware landscape is now more fragmented, unpredictable, and opportunistic than ever.



2025 Finance Report | blackfrio.com

Why Are Ransomware Attacks on Finance Down?

The financial sector is among the most heavily protected industries.

Breaching these systems is significantly more challenging due to several factors:

Sensitive Data and High Stakes

The data held by financial institutions is directly tied to money and highly sensitive customer information (e.g., bank accounts, credit card numbers, social security numbers). Significant and advanced security defenses protect these high-value assets.

Stringent Regulations and Compliance

Financial institutions operate under a vast array of strict regulations, such as those from the SEC, FINRA, and various international bodies. These regulations include cybersecurity practices, data protection standards, and incident reporting requirements.

Dedicated Security Resources

Financial companies typically employ Chief Information and Security Officers (CISOs) and dedicated security teams whose primary responsibility is to safeguard their systems and processes. This includes continuous monitoring, threat intelligence, and rapid incident response capabilities.

Government and Law Enforcement Collaboration

There's often close collaboration between financial institutions and government agencies to counter cyber threats. Major ransomware groups that historically targeted financial organizations have been actively dismantled by government agencies, making direct attacks harder and less appealing for newer or less skilled groups.

The ransomware business ecosystem has changed.

As we highlighted in our 2025 Ransomware Report, the dismantling of major and well-equipped ransomware groups like LockBit and AlphV led to fragmentation within the ecosystem. While these larger and more established groups poisessed the capability to target Financial Services companies, the smaller, less sophisticated groups that remain lack the same means to attack a well-protected industry.

In the absence of these larger groups, we now observe that Ransomware-as-a-Service (RaaS) tools are being sold for very low prices, typically between $100 and $1,000 per attack. This has opened the door for less experienced individuals to enter the ransomware scene. In fact, every day, new groups emerge and carry out attacks. But breaching financial defenses remains significantly more challenging. As a result, newer and less skilled groups often prefer to avoid targeting such high-security environments.

The Future of Ransomware Attacks on the Financial Sector

While direct attacks on the financial sector appear to be decreasing, this trend is not guaranteed to continue. The cyber threat landscape is highly dynamic, and attackers are quick to adapt. Smaller, less capable groups may evolve over time and become more organized.

With the increasing use of AI-powered automation tools, easier access to technical knowledge, and the growing availability of open-source exploit kits, even actors once considered "inexperienced" could gain the ability to conduct sophisticated attacks. Moreover, attackers may shift from targeting financial institutions directly to exploiting weaker links within their ecosystems.

This brings us to a critical point: third-party risk.

Finance's Vendors Pose a Greater Risk

Even though financial institutions have made significant progress in securing their own systems, vendor-related exposures remain a major concern. External service providers, software vendors, and infrastructure partners often serve as alternative, and more vulnerable, entry points for attackers.

Therefore, while the drop in direct attacks is promising, the risk of indirect access through third parties continues to pose a serious threat to the financial sector.

Let's look at the risks lurking in the financial sector's vendor ecosystem.

PREVIOUS NEXT

Finance Vendor Trends

Weak Links in the Financial Sector Supply Chain

The lack of ransomware activity directly on financial companies doesn't mean the sector is safe. We analyzed 140 vendors that primarily serve the financial sector. These vendors offer a wide array of services, including Professional, Scientific and Technical Services (NAICS 54), Computer Systems Design and Related Services (NAICS 5415), Software Publishers (NAICS 5112), and Manufacturing (NAICS 33).

Across 140 vendor companies, there are a lot of weaknesses out there that can impact your business. These companies don't have the same robust defenses and regulatory obligations as the financial industry. If these vendors are breached or experience system outages, the impact can be widespread.

Financial Sector's Vendor Risk Data

We looked at multiple factors that assess the cybersecurity of vendors in the financial sector:

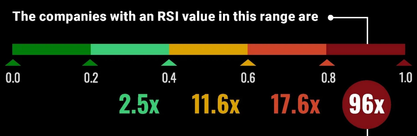
- Average Score: Ranging from 1-100, the Black Kite Technical Rating provides easy-to-understand letter grades and defensible data details behind 20 risk categories.

A	B	C	D	F
(Excellent)	(Good)	(Fair)	(Poor)	(Failing)
90-100	80-89	70-79	60-69	0-59

- Ransomware Susceptibility Index® (RSI™): On a scale from 0.0 to 1.0, Black Kite's RSI shows you which vendors are most likely to experience a ransomware attack.
- Data Breach Index (DBI): A rearview mirror of past breach incidents to provide historical context for vendor risk.
- Data Breaches: How many breaches occurred within the vendor set over the past 2 years.
- Critical Vulnerabilities (CVSS ≥ 8 and CVSS > 9): How many vendors are found to have the most critical CVEs.

POWER OF RSI

The companies with an RSI value in this range are



more likely to experience a ransomware attack than the companies with an RSI value below 0.2

Top 20 Vendors Serving Finance

85 (B) Average Score: 85 (B)	**0.387** Ransomware Susceptibility Index (RSI)	**0.144** Data Breach Index (DBI)
1 Data Breach	**10** Vendors Critical Vulnerabilities (CVSS ≥ 8)	**9** Vendors Critical Vulnerabilities (CVSS > 9)

All 140 Vendors Serving Finance

87 (B+) Average Score: 85 (B)	**0.437** Ransomware Susceptibility Index (RSI)	**0.136** Data Breach Index (DBI)
6 Data Breach	**31** Vendors Critical Vulnerabilities (CVSS ≥ 8)	**15** Vendors Critical Vulnerabilities (CVSS > 9)

We see some common and concerning risk issues and trends observed among the 140 vendors:

High Common Vulnerability Scoring System (CVSS) Ratings:

31 vendors have at least one critical vulnerability with a CVSS at or above 8, and 15 of those vendors show an extremely high risk with CVSS scores above 9.

Concerning RSI Levels:

The average RSI of 0.437 suggests a notable susceptibility to ransomware, which is particularly alarming for vendors supporting critical financial systems. Companies within this range are 11.6 times more likely to experience a ransomware attack than companies with an RSI below 0.2.

High Risk FocusTag™ Patterns:

Black Kite FocusTags™ give immediate visibility into the most concerning risks in your vendor ecosystem so you can take action. Among the 140 vendors serving the financial sector, 90 are flagged with high-risk threat categories, including 35 vendors marked with Known Exploited Vulnerabilities (KEV) tags, highlighting the active exploitation of the risks they face.

Oracle Data Breach

41 (29%) of the 140 vendors were tagged with an Oracle Data Breach FocusTag.

- This tag highlights vendors that experienced a compromise related to Oracle data, indicating potential exposure of sensitive information or vulnerabilities within cloud security infrastructures.
- Such breaches can have a cascading effect, as many organizations, including those in financial services, rely on Oracle Cloud for critical operations, making the security of their data within these cloud environments a key third-party risk management concern.

Cleo File Transfer

5 vendors were tagged with a Cleo File Transfer FocusTag.

- This tag indicates vendors affected by the exploitation of vulnerabilities in Cleo's Managed File Transfer (MFT) solutions by the Clop ransomware group.
- While Clop did not directly breach Cleo, they leveraged vulnerabilities in Cleo's widely used products (like Harmony, VLTrader, and LexiCom) to target companies in various supply chain operations, including those potentially serving the financial sector.
- The exploitation of MFT tools represents a significant supply chain risk, as these solutions are central to data exchange between organizations, and a compromise can lead to widespread operational disruptions and data exfiltration across interconnected businesses.

Case Study: Early Warning System Shields Company from Cleo Ransomware Impact

One company's rapid response, which was enabled by continuous third-party risk monitoring, allowed them to proactively defend against the impact of Clop's Cleo ransomware attack in their vendor ecosystem.

Company Profile

Based in United States with 340+ employees and annual revenue exceeding $240 million.

Initial Alert

Black Kite provided its first alert of a possible Cleo ransomware risk in the company's vendor ecosystem via the CLEO Integration - Ransomware Risk FocusTag™ on November 27.

Clop Ransomware Disclosure

The ClOp ransomware group disclosed the attack related to Cleo's exploited vulnerabilities three months later, on February 24.

Impact on TPRM

Black Kite's rapid tagging and risk assessment of the affected Cleo software enabled proactive defense measures for the company, demonstrating the value of timely third-party risk intelligence in mitigating potential supply chain fallout.

An example of FocusTags applied to a vendor in Black Kite's platform, highlighting the present risks.

CLEO Integration - Ransomware Risk

Ransomware | Data Breach

Oracle Cloud Data Breach | KEV

Key Vulnerabilities and Weaknesses in Finance's Vendor Ecosystem

Information Disclosure Risk

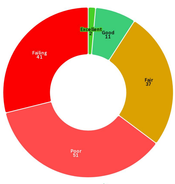
The financial sector depends on a broad range of third-party vendors to support key functions like infrastructure, compliance, and digital transformation. Alarmingly, **129 out of 140 vendors (92%) received a score of C, D or F in Information Disclosure**, indicating a systemic issue in how these companies manage and expose sensitive technical information.

The vulnerabilities uncovered include:

- Public exposure of employee email addresses (phishing risk)
- Disclosure of software version numbers (vulnerability mapping)
- WHOIS misconfigurations revealing personal data
- Indexing of private directories and error messages leaking system internals

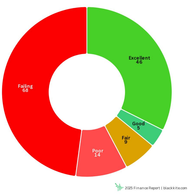
These are not "low-impact" issues. They provide a blueprint for attackers to plan phishing campaigns, target software-specific exploits, or map the vendor's infrastructure—all of which can cascade into financial institutions that depend on them.

Information Disclosure Scores for Vendors Serving Finance



Source: 2025 Finance Report | blackkite.com

Patch Management Scores for Vendors Serving Finance



2025 Finance Report | blackkite.com

Patch Management Weaknesses

Patch Management is perhaps the clearest window into an organization's operational maturity. Unfortunately, **half of the most widely used vendors in the financial supply chain are still operating outdated or legacy systems**.

5This indicates that **65% of vendors are not maintaining current patch levels**, which exposes financial institutions to inherited risk from known CVEs and potentially unpatched zero-day vulnerabilities in legacy technologies.

This is particularly dangerous because **financial institutions may be compliant themselves, yet still be indirectly vulnerable** through service providers that do not patch actively or still rely on deprecated systems like IIS/7.5, Apache Struts, or outdated OpenSSL libraries.

Application Security Exposure

Web applications form the primary interface between vendor systems and their clients—including financial organizations. Weak application security often results in **exploitable login flows, session mismanagement, and improper encryption practices**.

Roughly **1 in 5 vendors still operate with major application-layer weaknesses**, such as:

- Cleartext transmission of sensitive information
- Missing CSRF tokens
- Improper HTTP headers
- No brute-force or bot detection on login pages

For vendors providing services like client portals, reporting dashboards, and cloud-based finance apps, these weaknesses can **serve as a direct entry point to financial systems and data**.

Application Security Scores for Vendors Serving Finance

Source: 2025 Finance Report | blackkite.com

Credential Management Exposure

Credential leaks remain one of the **most commonly exploited weaknesses in ransomware and phishing attacks**. Encouragingly, only **7 of the 140 vendors received D–F scores**, indicating that most vendors have **acceptable practices in place for account hygiene**.

However, given their high-profile clients in the finance sector, even a **single compromised employee credential** can enable attackers to escalate privileges or perform reconnaissance across sensitive systems.

This relatively strong performance suggests improved employee awareness and password hygiene, but it must be continuously monitored. **Leaked credentials can appear months after a breach**, and the absence of recent findings does not always imply security.

Credential Management Scores for Vendors Serving Finance

7

D-F

133

A-B

Hacktivist Activity Scores for Vendors Serving Finance

13

D-F

127

A-B

Hacktivist Shares

Hacktivist chatter is a proxy for reputation, visibility, and perceived weakness. **13 vendors were mentioned in dark web or underground forums with D–F grades**, typically indicating leaked documents, exposed credentials, or direct mentions of their brand or infrastructure.

Even if these mentions don't always involve active exploits, they signal **intent and targeting from ideologically motivated or opportunistic attackers**. Financial institutions using these vendors should pay special attention to third-party threat intelligence alerts.

Extended Risk Intelligence: Control-Based Findings

While category-level grades offer a broad view of vendor security posture, individual control failures reveal specific, targeted weaknesses that attackers actively exploit. For vendors most relied upon by the financial industry, these control-level findings highlight systemic risks across phishing, outdated infrastructure, and credential exposure.

Stealer Log Records

Finding: 39 vendors had **employee credentials found in stealer logs**

Credential data harvested from information-stealing malware often appears months after the initial compromise and frequently includes access tokens or passwords for internal services.

Vendors with stealer data present a **clear lateral movement risk** if connected to critical bank infrastructure.

Missing DMARC Records

Finding: 19 out of 140 vendors lack a DMARC record

Without a valid DMARC (Domain-based Message Authentication, Reporting & Conformance) policy, vendors are susceptible to domain spoofing and phishing attacks.

This allows attackers to impersonate these vendors in emails—**undermining trust with financial institutions and their clients**.

DNS Amplification

Finding: 51 vendors are **vulnerable to DNS amplification DDoS** attacks

These systems can be abused as reflectors in volumetric DDoS (Distributed Denial of Service) attacks—either as victims or as unintentional participants.

This is especially concerning for **cloud-hosted services** used by multiple financial clients, risking service degradation or takedown.

Outdated / End-of-Life Systems

Finding: 31 vendors run **end-of-life or unsupported systems**

EOL systems do not receive patches and violate most data protection regulations. They are also disproportionately targeted by attackers due to accumulated vulnerabilities.

Continued reliance on EOL technologies in the financial supply chain is **a ticking time bomb for compliance and integrity**.

Data Breach Exposure

Finding: 20 vendors are tied to previous data breaches

This metric highlights organizations with known data exposure histories—indicating weak historic security programs and a possible **pattern of failure**.

These vendors are more likely to experience repeat compromises unless they've demonstrably hardened their infrastructure.

Bot Attack Weakness

Finding: 30 vendors lack **controls for brute-force or bot attacks on login forms**

This allows attackers to attempt password stuffing or DoS tactics against login interfaces, increasing the risk of unauthorized access.

For vendors with authentication services or financial logins, this is an **unacceptable entry vector**.

Cross-Site Request Forgery

Finding: 14 vendors are vulnerable to CSRF

CSRF flaws enable attackers to **trick authenticated users into executing actions without their intent**. For instance, changing user data, modifying permissions, or initiating transactions.

If exploited, CSRF in a vendor's system could propagate fraudulent actions back into banking systems.

Phishing Domains

Finding: 40 vendors are linked to **phishing domains or suspicious URLs**

Black Kite threat intel crawlers detected the use of vendor brands or URLs in phishing campaigns—posing serious reputational and impersonation risks.

These vendors are **already being exploited in the wild** to deceive end users or target institutions.

These are not isolated issues.

These findings are not outliers. They are symptoms of deeper, systemic fragility. When 28% of vendors have employee credentials circulating in stealer logs, 22% still run outdated systems, and 36% can be abused for DDoS attacks, the conclusion is clear: the security posture of the financial sector's extended ecosystem is crumbling.

No matter how well-defended a financial institution may be, a single exposed partner becomes the weak link that attackers exploit. Phishing domains, end-of-life technologies, bot-exploitable logins – these aren't future threats. They're present realities.

If financial institutions don't act now by auditing, pressuring, and even replacing underperforming vendors, they're not just managing risk, they're absorbing it.

The perimeters have shifted. And so must the defense strategy.

Let's see what can happen if one of these weaknesses results in a breach.

PREVIOUS NEXT

Widespread Impact

When Vendor Breaches Ripple Through the Financial Ecosystem

A cybersecurity incident, or even a systemic outage at a single vendor, can send shockwaves throughout the interconnected financial ecosystem. Even the most secure financial institutions are vulnerable if a critical third-party service provider experiences disruption, underscoring the critical importance of a comprehensive supply chain risk management strategy.

The following examples highlight how vulnerabilities and disruptions in the vendor landscape can have widespread, cascading effects on financial services.

Case Study: Snowflake Cloud Data Platform Compromise Impacts Major Financial Clients

Overview:

- In 2024, Snowflake, a leading cloud-based data warehousing platform, became the epicenter of a series of high-profile compromises affecting its clients and their downstream ecosystems due to unauthorized network access.
- This incident revealed a significant gap in the adoption of essential security controls, particularly multi-factor authentication (MFA), and highlighted the need for continuous monitoring to detect early signs of unauthorized activity.
- Experts noted that a lack of robust detection mechanisms could have flagged unauthorized access earlier in the attack chain, emphasizing the necessity of comprehensive security measures in cloud environments.

Attack Details:

- Attackers leveraged infostealer malware to compromise credentials, gaining unauthorized access to Snowflake accounts that lacked multi-factor authentication (MFA).
- The breach resulted in data exposure for Snowflake's customer organizations, collectively impacting millions of individuals.
- Technical analysis revealed that many of the compromised credentials had been harvested through prior malware infections and traded on dark web forums.
- Attackers exploited these stolen credentials to access sensitive datasets stored within the Snowflake platform, including financial information, operational data, and customer records.

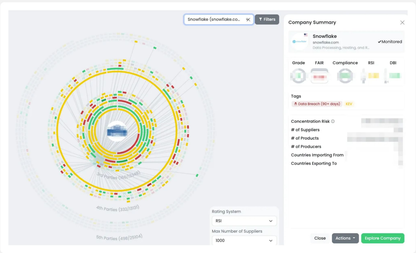
Impact on Financial Services:

- The compromise had extensive downstream effects across the financial sector.
- Santander Bank and LendingTree were among the affected financial clients, requiring rapid incident response and communication strategies to mitigate the risk of fraud and identity theft for their customers.
- The incident underscores how a vulnerability in a single widely-used platform can create significant ripple effects, extending risk far beyond the initially compromised service.

Lessons Learned:

- The Snowflake breaches serve as a stark warning about the cascading risks inherent in cloud-based ecosystems.
- Organizations relying on third-party platforms must adopt stringent security practices, including mandatory MFA for all accounts, regular credential hygiene, and proactive, continuous monitoring of their cloud environments.
- These measures are vital to safeguarding against credential-based attacks that exploit the pervasive interconnectivity of modern supply chains.

Black Kite's Supply Chain shows users where Snowflake is being used throughout their Nth-party ecosystem:



Case Study: Cleo Managed File Transfer Exploitation Causes Supply Chain Disruptions

Overview:

- Following the Blue Yonder attack, vulnerabilities in **Cleo's** Managed File Transfer (MFT) solutions became a significant focus of exploitation by the Cl0p ransomware group.
- It is critical to clarify that Cl0p did not breach Cleo directly but leveraged vulnerabilities in Cleo's widely used products, such as Harmony, VLTrader, and LexiCom, to target companies relying on these solutions for supply chain operations.
- This campaign mirrors Cl0p's previous exploitation of MOVEit and GoAnywhere products, highlighting their focus on systemic vulnerabilities in Managed File Transfer tools.

Attack Details:

- The exploitation began in December 2024, with Cl0p actively targeting companies using unpatched versions of Cleo's MFT products.
- The group utilized a combination of CVE-2024-50623, allowing unrestricted file uploads and remote code execution, and CVE-2024-55956, a zero-day vulnerability enabling data exfiltration.
- By December 13, Cl0p publicly claimed responsibility, listing 66 victims on their dark web extortion site.
- Researchers estimated that the actual number of impacted organizations could be in the hundreds, given Cleo's widespread adoption in industries like retail, logistics, and manufacturing.

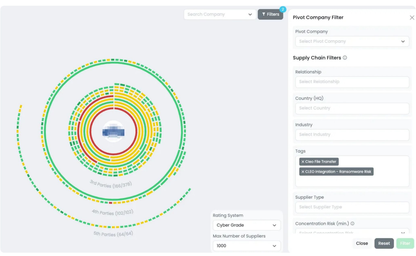
Impact on Financial Services-Related Supply Chains:

- The exploitation resulted in operational disruptions across various sectors linked to financial supply chains.
- Retailers faced delays in shipment tracking and inventory management, while manufacturers reported production halts and increased downtime due to compromised integrations.
- These disruptions highlight how an attack on a software tool can have far-reaching consequences for the entire operational flow of businesses that are integral to the financial ecosystem.
- Organizations using Cleo's products were urged to prioritize immediate patching to version 5.8.0.21 or later, implement stricter access controls, and enhance monitoring for Indicators of Compromise (IoCs).

Lessons Learned:

- This ongoing campaign emphasizes the urgent need for proactive vulnerability management and robust supply chain risk assessments.
- Organizations must collaborate closely with their third-party vendors to address known vulnerabilities swiftly and implement strong defensive measures to ensure resilience in interconnected ecosystems, preventing single points of failure from causing widespread disruption.

Black Kite's Supply Chain shows our users their Nth-party ecosystem filtered by Cleo FocusTags™:



Case Study: Fiserv Widespread Banking Outage Disrupts Services Across U.S.

Overview:

- In a stark reminder that not all significant disruptions are cyberattacks, financial institutions operating in the United States experienced widespread outages following a service disruption at financial technology provider **Fiserv** on May 2, 2023.
- This incident, while not a cyber event, led to significant impairment across multiple banks and credit unions, affecting their ability to deliver critical banking services to customers.

Incident Details:

- Fiserv supplies the infrastructure behind many major financial institutions' digital platforms.
- Banks affected included major players such as Ally, Bank of America, TD Bank, Capital One, Synchrony, and Citizens Bank, as well as regional and local institutions like Northwest Bank, Sunflower Bank, and Farmers National Bank in Ohio.
- Credit unions such as Navy Federal were also impacted, and even money transfer service Zelle appeared to be affected.
- The outage occurred during a planned "enhancement" of the network infrastructure at a Fiserv data center.

Impact on Financial Services:

- The widespread nature of the outage meant that critical banking services, such as account access, fund transfers, and payment processing, were unavailable to a vast number of customers.
- While the issue was resolved within a day, the incident underscored the profound interconnectedness and fragility of modern financial infrastructure.
- It demonstrated that even an operational glitch at a single, critical third-party provider can bring significant portions of the financial ecosystem to a standstill, causing inconvenience to millions and raising concerns about resilience.

Lessons Learned:

- This event highlights that "supply chain risk" extends beyond traditional cyber threats to include operational failures or technical issues at key service providers.
- Financial institutions must assess and plan for disruptions from all types of vendor incidents, ensuring redundant systems and robust continuity plans are in place for critical third-party dependencies.
- It reinforces that a strong defense is not just about preventing malicious attacks, but also about preparing for any event that can compromise the availability and integrity of services delivered through the supply chain.

Learn how to see risk in your vendor ecosystem to protect your organization.

PREVIOUS NEXT

Next Steps for Proactive Vendor Risk Management

The evolving cyber threat landscape, where direct ransomware attacks on financial institutions have declined but risk from the vendor ecosystem is growing, demands a proactive and comprehensive approach to cybersecurity. Financial institutions can no longer afford a false sense of security based solely on their internal defenses. The real challenge lies in mitigating the "hidden dangers" within their supply chain.

To effectively address these vulnerabilities and protect critical operations, financial services organizations should implement the following strategic steps:

Enhance Visibility into the Nth-Party Ecosystem

A fundamental first step is to gain clear and continuous visibility into the entire third-party and Nth-party vendor ecosystem. Many organizations have an incomplete picture of their digital supply chain, making it impossible to manage risks effectively.

Understanding every entity that contributes to critical operations, from software providers to cloud infrastructure partners, is paramount.

Prioritize and Assess Vendor Risk Continuously

Not all vendors pose the same level of risk. Financial institutions must prioritize vendors based on their criticality to business operations and the sensitivity of the data they handle. Continuous monitoring and assessment, rather than point-in-time questionnaires, are essential for identifying emerging vulnerabilities in real-time.

Focus on Key Vulnerability Areas

As highlighted in this report, specific weaknesses and critical vulnerabilities (CVEs) are prevalent across the financial sector's vendor ecosystem. Financial institutions must move beyond a generalized understanding of risk to actively prioritize and push for the remediation of the most dangerous CVEs impacting their third parties, as these vulnerabilities are actively being exploited and represent an imminent threat.

Understand Vendor Susceptibility to Ransomware

It's crucial for financial institutions to assess not just the general security posture of their vendors, but specifically their susceptibility to ransomware attacks. Leveraging objective, data-driven insights to understand the likelihood of a vendor experiencing a ransomware incident allows organizations to identify high-risk vendors and understand where their supply chain might be most vulnerable to the very attacks they are well-defended against directly.

Knowing which vendors pose a higher risk in terms of ransomware susceptibility enables targeted risk mitigation and strategic planning for potential disruptions.

Collaborate Closely With Vendors to Resolve Risk

Effective remediation of identified risk requires active collaboration. Financial institutions should not merely present vendors with a list of issues, but work collaboratively to address identified vulnerabilities and weaknesses. This includes sharing defendable intelligence and fostering a shared understanding of the importance of security the supply chain.

Utilizing platforms that facilitate secure communication and streamline remediation processes can significantly improve the speed and effectiveness of risk resolution across the vendor ecosystem.

By adopting a proactive, intelligence-driven approach to vendor risk management, financial institutions can move beyond a false sense of security and genuinely strengthen their cybersecurity posture against the evolving landscape of threats, protecting their assets, their customers, and the stability of the broader financial ecosystem.

Learn more about how Black Kite helps you stay on top of your cyber ecosystem risk.

Request a Demo

Methodology of the Report

The data presented in this report is the result of a multi-source, intelligence-led investigation by the **Black Kite Research & Intelligence Team (BRITE)**. It synthesizes extensive threat intelligence, ransomware tracking, vendor ecosystem analysis, and cyber risk telemetry to provide a comprehensive view of systemic third-party vulnerabilities in the financial sector.

1. Data Sources and Scope

This report integrates several streams of intelligence curated by BRITE between **January 2023 and May 2025**. The ransomware-related data specifically includes only confirmed victims where both encryption and data leaks were verified, and attribution to a known ransomware group was clearly established.

All vendor-related data was derived from Black Kite's proprietary telemetry and publicly available information, supplemented by intelligence gathered from surface, deep, and dark web sources.

2. Industry Classification and Exclusions

To maintain analytical consistency, **industry classifications were aligned to NAICS (North American Industry Classification System) codes**. While 52 NAICS codes were reviewed, the code **524 (Insurance Carriers and Related Activities)** was deliberately excluded from the final figures due to its structural and regulatory segmentation. However, entities under **5251 (Insurance and Employee Benefit Funds)** were included, as they represent financial investment mechanisms rather than insurance providers.

3. Company Size and Risk Posture Analysis

For each entity—victim or vendor—BRITE analysts estimated company size using **public financial disclosures, reliable third-party databases, and organizational benchmarks**. In addition, the **Black Kite platform** was used to assess and track each organization's **cybersecurity posture before and after ransomware incidents**, enabling comparative analysis of susceptibility factors and exposure levels.

4. Vendor Selection Criteria

The core of this report focuses on a **targeted analysis of 140 vendors** serving the financial sector. Selection was made based on a unique criterion: **Vendors whose client base includes at least 10% financial sector customers**, regardless of company size. This ensured that the analyzed vendor pool reflected high relevance and potential impact on the financial services supply chain.

5. Standardization and Integrity Controls

To ensure consistency and prevent data inflation, BRITE applies a **standardized victim counting methodology**. For example, attacks targeting clinic chains, dealer networks, or holding structures are counted as a single incident unless distinct disclosures exist.

6. Technical Ratings Explained

The Black Kite Technical Rating ranges from 1 to 100 and covers 20 risk categories. Scores are also translated into letter grades for clarity:

- A (Excellent): 90–100
- B (Good): 80–89
- C (Fair): 70–79
- D (Poor): 60–69
- F (Failing): 0–59

7. Limitations

This report reflects only **publicly disclosed ransomware incidents and observable vendor risk indicators**. Many breaches—especially those involving smaller entities or resolved discreetly—go unreported. Consequently, the findings represent a **conservative lower bound** of systemic third-party risk exposure.

PREVIOUS PAGE