RaNSOMw IN THE FINANCIAL

Financial Institutions Are Ransomware Sector Targets: What to Know and How to Respond

BY LUKE DEMBOSKY AND JORDAN RAE KELLY

Financial Institutions (FIs) hold vast amounts of sensitive customer data, manage substantial funds, and operate in an ever-expanding digital environment, making them a prime target for threat actors.

Given this threat, FIs must be vigilant against sophisticated threat actors like Scattered Spider. Scattered Spider is a notable example of a sophisticated ransom threat actor group that has successfully and increasingly targeted organizations in the financial services industry. The group has deployed tactics such as calling IT Help Desks while impersonating an employee and requesting a password reset, thereby obtaining legitimate credentials and gaining access to an organization's network. Scattered Spider also sends lookalike domains and phishing emails to direct employees to fake login pages.[1] Once an employee enters their login information into these fake websites, the group steals the user's credentials.

Ransomware attacks in the financial services industry, perpetrated by groups like Scattered Spider and numerous others, have surged dramatically. In 2023 alone, the industry experienced a 64 percent increase in such attacks.[2] This increase is likely due to the significant disruption ransomware attacks can cause to the operations of FIs.

Given the substantial risk posed by ransomware attacks, cybersecurity is a shared responsibility across an entire organization, not just confined to information technology (IT) teams. The far-reaching impact of a ransomware attack on all departments in an organization necessitates that stakeholders and leaders must play a vital role in understanding, mitigating, responding to, and recovering from such incidents. This need to prepare for the threat of ransomware by building cyber resilience—the ability to respond to an attack immediately and resume operations quickly—is imperative to minimize downtime and negative impacts.

What is Ransomware?

At a high level, ransomware is malicious software used by threat actors that blocks access to, or encrypts, networks until these criminals are paid a requested sum of money. Ransomware attacks are increasingly costly to organizations, with the average cost reaching $5.13 million in 2023. This figure is a 13 percent increase from last year and does not include the cost of the ransom payment itself.[3] As strengthening cybersecurity continues to be a top priority for organizations and more resources are being dedicated to mitigate ransomware attacks and associated costs, threat actors have evolved their tactics to pressure organizations into making ransom payments.

A double extortion ransomware incident occurs when, in addition to encrypting systems, threat actors also steal data, such as sensitive client information like credit card and social security numbers, and restricts access to it. They then threaten to expose this information by publishing the data on the dark web if the ransom is not paid, adding a second point of leverage to their pressure campaign.

Some threat actors now skip encryption and focus on stealing data, demanding payment to "delete" or not publish it. This method generally requires less technical skill by avoiding the need to deploy ransomware at scale, and instead simply exploits the victim's fear of sensitive or proprietary information being leaked, which can damage reputation, lead to financial losses, or increase the risk of litigation. Some actors take the attack a step further through triple extortion incidents. These incidents occur when threat actors apply additional pressure by threatening employees, customers, and partners of an organization, or by making the attack publicly known. Recently, threat actors have leveraged compliance requirements, such as those from the Securities and Exchange Commission (SEC) that require covered publicly traded companies to report material cybersecurity incidents within four business days.[4] These criminals have been known to apply significant pressure to organizations by preemptively notifying a regulator of the breach before the victim can report the incident themselves. This can force a victim's hand

on regulatory filings and public statements, and thereby pressures organizations to pay the ransom rather than incur regulatory scrutiny and possible fines, in addition to reputational damage. Additionally, it's important to note the significance of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). When it goes into effect late next year, CIRCIA will require organizations to notify the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours of making a ransomware payment.[5] This regulatory development underscores the critical need for timely reporting and enhances the collective effort to combat ransomware attacks.

Ransomware attacks at all levels of extortion are often carried out by large, organized groups like Lockbit, Black Basta or Scattered Spider. While these groups are highly sophisticated, it is becoming easier for other cyber criminals with fewer technical skills to exploit organizations for ransom with Ransomware-as-a-Service (RaaS) products. Large threat actor groups sell their malicious software variants as another stream of profit, meaning that criminals no longer need technical acumen to carry out their own attacks.

Given the substantial risk posed by ransomware attacks, cybersecurity is a shared responsibility across an entire organization, not just confined to information technology (IT) teams.

How Ransomware Attacks Happen

In order for a threat actor group to deploy ransomware, they must first gain access to an organization's network. Sophisticated ransomware groups have specialized methods for infiltrating organizations to deploy ransomware. There are several avenues that can serve as initial access vectors, but overall, existing vulnerabilities and poor cybersecurity hygiene practices make it significantly easier for threat actors to infiltrate networks.

- *Social Engineering:* By relying on human interaction, threat actors manipulate employees into unwittingly providing their credentials or other sensitive information through tactics like phishing emails and realistic scam and help desk phone calls. Threat actors can then access networks with the legitimate credentials they were able to obtain.
- *Internet-Facing Vulnerabilities:* Threat actors often exploit unpatched vulnerabilities in organizational networks to access networks through "backdoors" without credentials. These vulnerabilities can result from neglecting to update to the latest version of software, using outdated applications, or inadequate cybersecurity protections and monitoring.
- *Compromised Credentials:* Threat actors can compromise user credentials to access systems when accounts are not properly protected. This can include exploiting weak passwords or those obtained from third parties, particularly where no multi-factor authentication (MFA) is enabled.
- *Third Parties:* Many organizations use third-party providers for cloud storage, software needs, and other services that require the vendor have access to organizational networks. If these vendors do not have proper cybersecurity protections in place, threat actors can gain access to their target victims by way of third parties.

Once a threat actor gains access to a network and deploys ransomware, organizations must often pay the ransom or decrypt the decryption code to unlock their data. Ransomware decryption is a difficult, technical, and laborious process that often requires assistance from external experts. In certain instances, law enforcement may have decryption information available to assist. Other times, organizations may have no other option but to pay the ransom to resume operations or prevent sensitive information from being leaked, even with certain risks associated with making a payment. Because making ransom payments does not address the underlying vulnerabilities that allowed the threat actor to gain access into internal systems, organizations must still conduct thorough forensic investigations to find and eradicate "back doors" and other means of unauthorized access.

Why FIs are Targeted

Ransomware threat actors are financially motivated, but some, particularly those associated with hostile nation-states, are also focused on inflicting harm, causing chaos, and funding other illicit activities. For these reasons, threat actors are increasingly selective in who they attack, often choosing organizations that are most likely to pay. This makes critical infrastructure sectors like financial services a popular target because of the severe disruption that would be caused by losing access to systems. FIs, eager to restore their networks back and avoid harming consumer trust and stakeholder confidence, are more likely to pay to quickly restore operations. One in ten of the ransomware cases reported to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) for critical infrastructure sectors in 2023 were from financial services organizations.[6]

Because of their large and multi-faceted network environments, FIs generally present more surface area for potential network intrusions than many other industries, making the challenge of defending them all the greater. Legacy technology is still crucial to operations at many financial institutions because of the cost and time it takes to integrate new systems, but this outdated technology often lacks the proper safeguards to prevent ransomware attacks effectively. Legacy systems combined with a push for increased digitization of services from customers often results in a reliance on third-party providers for digital operations, creating a larger attack surface and additional pathways for entry for threat actors. The financial services industry is also highly regulated, with an increased focus on cybersecurity from many regulators like the New York Department of Financial Services (NYDFS). These potential regulatory ramifications place further pressure on organizations during and after ransomware attacks.

How to Respond in the Event of a Ransomware Incident

When a ransomware attack occurs, relevant stakeholders must be prepared to respond immediately. Outside of the technical response required from IT and cybersecurity teams, broader crisis management capabilities are essential to ensure an attack can be mitigated with as little damage as possible.

Ransomware attacks severely hinder access to organizational systems and networks, so operations teams will need to evaluate how business can continue while the incident is being handled. Following are some questions to ask.

- Does the organization have adequate backup data sets that can still be accessed?
- Are there ways to continue operating without severely disrupting customers and incurring significant financial repercussions?
- Regarding the additional extortion threat related to data theft, does the organization have strong data governance?
- Does this data governance plan including data minimization and least-privileged access management, along with data loss prevention controls, to reduce data surface area?

Risk, compliance, and legal teams should determine any regulatory deadlines that need to be met for incident reporting requirements and ensure all company and industry crisis protocols and policies are followed.

Crisis communications teams will also be valuable in responding to a ransomware incident to determine if, when, and how customers, investors, and the board of directors should be notified of the incident. Should the incident become public, they can also navigate media commentary to reduce the negative reputational impact of the incident. These teams are also integral for preparing emergency internal communications, to address issues such as harassment of employees, which is becoming increasingly prevalent in ransom attacks.

Engaging with law enforcement as early as possible during a ransomware attack can decrease the length and financial impact of the incident. According to IBM's Cost of a Data Breach Report, the total time to identify and contain a ransomware incident in 2023 was 33 days shorter when law enforcement was engaged, and total costs were reduced from $5.11 million to $4.64 million with the assistance of law enforcement.[7] When a ransomware incident is reported to the FBI, agents are able to provide information on decryption, assist in the recovery of stolen data, possibly recover ransom payments, and use the information gained from the incident in their efforts to dismantle ransomware groups.

Once an incident is contained, post-incident recovery efforts will include investigating the root cause of the incident and subsequently remediating any issues that allowed for initial network access by the threat actor. Security teams will likely continue monitoring the dark web to assist in determining whether and what data was compromised. As recovery progresses, it is necessary to keep both internal and external stakeholders informed of any compromised data, the remediation actions being taken, and the financial and operational impact of the incident to the organization.

Cyber risk insurance policies often outline specific procedures that a company must follow in response to a cyber incident, including ransomware attacks. These policies typically dictate how the company should respond, the timeline for reporting the incident, and the approved providers that must be used for services such as forensic investigations. Compliance with these policy requirements is essential for ensuring coverage and support during a ransomware incident, thereby helping to mitigate financial and operational impacts.

Legal and Regulatory Considerations

The cybersecurity regulatory landscape for the financial services industry constantly evolves as regulators release new and updated rules to protect organizations and customers alike. These regulations involve standards for incident prevention and requirements for notifying stakeholders and customers after incidents. Fines from regulators, legal fees, and the resources required to remediate and rebuild after incidents can be a significant financial burden on an organization. As a result, regulatory factors play a significant role in mitigating ransomware attacks and in cybersecurity incident prevention and response.

- *SEC Cybersecurity Rules:* The SEC cybersecurity rules for issuers,[8] which became effective on December 18, 2023, require public companies to comply with cybersecurity disclosure guidelines, including disclosing "material" incidents within four business days. The rules also require more transparency into organizational cybersecurity practices, such as documentation outlining how the board oversees and is informed about cyber risk, and how the organization identifies, assesses, and manages material cyber risks.
- *SEC Amendments to Regulation S-P:* On May 16, 2024, the SEC announced amendments to Regulation S-P, designed to keep pace with how financial institutions use technology to manage customer information and other new digital risks.[9] The update requires broker-dealers (including funding portals), investment companies, registered investment advisers, and transfer agents to provide notice no more than 30 days after an incident involving unauthorized access to or use of customer information occurs.
- *FTC Safeguards Rule:* Amendments to the FTC Safeguards Rule took effect on May 13, 2024, requiring all financial institutions, including non-banking institutions such as mortgage brokers and payday lenders, to develop, implement, and maintain a comprehensive cybersecurity program.[10] The amendments also require that security breaches involving more than 500 customers be disclosed to the FTC less than 30 days after discovery.
- *New York Department of Financial Services (NYDFS) Part 500 Cybersecurity Rules:* Published November 1, 2023, updates to the NYDFS Part 500 Cybersecurity Rules made several additions to cybersecurity expectations of financial institutions operating in New York.[11] This includes regular, independent audits of cybersecurity programs, executive approval of cybersecurity policies, written policies and procedures surrounding third-party providers, and notification no later than 72 hours after a cybersecurity incident has occurred.
- *CISA's Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA):* CIRCIA would require critical infrastructure entities, including financial

institutions, to report certain cybersecurity incidents within 72 hours, and ransomware payments within 24 hours.[12] CISA expects to publish the final rule no later than October 4, 2025.

- *Computer-Security Incident Notification Rule:* Issued by the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC), this rule mandates that banks report significant computer-security incidents to their primary federal regulator within 36 hours of discovery. It includes incidents such as a ransomware attack that encrypts core banking system/backup data of a bank.
- *Sanctions Risks and OFAC Guidance:* When addressing ransomware incidents, it is crucial to consider the potential sanctions risks associated with transactions involving unknown or possibly foreign bad actors. The Office of Foreign Assets Control (OFAC) has provided critical guidance on this issue, emphasizing that facilitating ransomware payments on behalf of a victim may violate OFAC regulations.
- Financial institutions and companies must exercise due diligence to ensure they are not inadvertently engaging with sanctioned entities or individuals. OFAC's guidance underscores the importance of understanding and complying with these regulations to avoid severe penalties.[13]

It is becoming easier for other cyber criminals with fewer technical skills to exploit organizations for ransom with Ransomware-as-a-Service (RaaS) products. Large threat actor groups sell their malicious software variants as another stream of profit, meaning that criminals no longer need technical acumen to carry out their own attacks.

Preventative Measures to Mitigate Ransomware Risks

Financial services organizations can mitigate the risk of ransomware attacks through robust cybersecurity programs, strong data governance, thorough incident response preparedness plans, and an understanding of the latest ransomware threats and tactics targeting the industry.

When responding to a ransomware attack, it is imperative to understand organizational policy surrounding ransom negotiation and payment. Some organizations have policies forbidding the payment of ransoms, while others will pay a ransom if necessary to restore critical systems or to prevent sensitive data from being leaked. While organizations that paid the ransom during an attack reported a small difference in average cost of responding to the incident ($5.06 million compared to $5.17 million in 2023), this does not include the cost of the ransom payment itself.[14]

An incident response plan should include the roles and responsibilities of all relevant internal stakeholders, such as IT, legal, compliance, general counsel, public relations, and the C-suite. It should also include necessary external parties such as cyber insurance providers, legal counsel, law enforcement, and any third-party response firms. Ransom payment policy information should be included as part of a comprehensive incident response plan, although one discretely held by the legal team. These types of response plans are an essential part of any organization's cybersecurity strategy because they outline the many strategic decisions that need to be made quickly during an incident. It is much more challenging to make thoughtful, time-sensitive decisions under pressure, so planning for them ahead of time will alleviate some of the stress that comes with an incident and facilitate a more efficient recovery.

The most effective way to ensure all relevant parties understand their role during a ransomware attack is to hold a cyber incident response simulation exercise, or a "tabletop." Running through a realistic ransomware scenario with team members, practicing crisis management, and testing the effectiveness of an incident response plan will instill confidence in capabilities and allow for the discovery of any gaps in the plan. Many organizations run cyber tabletop exercises on a regular basis, developing the scenarios internally, while periodically using outside experts—law firm cyber teams or technical incident response vendors or both—to design and facilitate realistic exercises to test first responders up through core response team and senior leadership on their ability to manage a cyber crisis.

Even employees not directly involved in incident responses play a role in mitigating the threat of ransomware. Social engineering tactics can be used by threat actors against any level of employee to gain access to systems, so it is imperative that organizations have policies, best practices, and training in place to protect employees against social engineering attacks and teach them to be cyber-aware. Employees should be cognizant of the psychological tactics that could be used against them by threat actors, and help desk staff should be trained to recognize signs of social engineering and verify identities before granting access to accounts.

Training programs should address longer-running threats like phishing emails by creating authentic and believable test phishing campaigns distributed to employees for evaluating awareness of social engineering threats. In addition, training programs should also include Help Desk manipulation, deepfakes, and other emerging threats targeting employees to gain network access or to initiate wire transfers.

Future Outlook and Emerging Trends

Ransomware threats constantly evolve, with new technologies providing threat actors with additional tools to carry out their attacks, and advances in cybersecurity protections forcing threat actors to become more creative with their methods. Following are several emerging threats and trends within the financial services industry that could impact the evolution of ransomware threats.

STOCK.ADOBE.COM / DELTA AMPHULE

- Black-Hat Generative AI Tools:[15] The advent of generative artificial intelligence (AI) technologies has brought about the development of AI chatbots specifically intended for malicious purposes that have been listed for sale across dark web marketplaces, offering an "alternative" to AI chatbots designed to operate under strict ethical limitations. These tools are specifically designed to create deepfakes, spread misinformation, access dark web sources, and easily write malicious code.
- Zero-Day Exploits: Zero-day attacks occur when a threat actor leverages an unknown software or hardware vulnerability, and a patch does not yet exist. These types of exploits have increased in recent years and provide an additional access vector for ransomware threat actors.
- Cloud Security: As more financial services organizations integrate cloud environments into their networks, threat actors have escalated their attacks on cloud platforms by exploiting vulnerabilities through user account takeovers, misconfigurations, and third-party vendors. Insecure cloud environments pose threats to organizations, whose networks and systems can be infiltrated, and to consumers, whose personal information is at risk of being compromised.

Ransomware attacks present a growing and persistent threat to organizations in highly targeted industries like financial services. Mitigating the evolving cyber risks surrounding sophisticated threat actors requires dedicated resources, comprehensive planning, training and testing, and active involvement from leadership across departments. ■

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates or its other professionals.

ABOUT THE AUTHORS

LUKE DEMBOSKY co-chairs Debevoise & Plimpton's global Data Strategy and Security practice, advising companies on managing cyber risks, responding to incidents, and handling related internal investigations and regulatory defense matters. He is ranked Band 1 by Chambers both for Privacy and Data Security and for Crisis Management.

Prior to joining Debevoise, Mr. Dembosky served as Deputy Assistant Attorney General for National Security at the U.S. Department of Justice, where he oversaw national security cyber cases; Deputy Chief at DOJ's Computer Crime and Intellectual Property Section; and DOJ's attache based at the U.S. Embassy in Moscow, where he served as the Department's representative to the Russian government on cyber and other transnational crime matters.

In his respective public and private sector roles, Mr. Dembosky has played a key role in responding to major cyber incidents, including those involving SolarWinds, NotPetya, Target, Sony Pictures, Home Depot, Anthem, and OPM. He received the Attorney General's Distinguished Service Award for leading the operation to dismantle the GameOver Zeus botnet, and represented DOJ in cyber negotiations with Russia and China. Reach him at **ldembosky@debevoise.com** or **linkedin.com/in/lukedembosky/**.

JORDAN RAE KELLY is a Senior Managing Director and the Head of Cybersecurity for the Americas at FTI Consulting (**fticonsulting.com**), with more than 15 years of experience in incident response and cyber policy planning. At FTI Consulting, she advises clients on cybersecurity and data privacy issues, including breaches, insider threats, intellectual property, crisis communications, vendor management, compliance, regulation, risk management, and forensic investigations.

Prior to FTI Consulting, Ms. Kelly served as the Director for Cyber Incident Response on the National Security Council at the White House, overseeing national incident response coordination and managing the U.S. Government's process for zero-day exploits. She was a chief author of the National Cyber Strategy, the first in 15 years.

Before joining the National Security Council, Ms. Kelly was the Chief of Staff and Chief of Strategic Initiatives in the FBI's Cyber Division, managing operations and policy planning for the FBI's national cyber program. She also worked as a law clerk in the Office of General Counsel at the Y-12 National Security Complex.

Ms. Kelly has been recognized in Consulting magazine's inaugural Women Leaders in Technology list and Global Investigation Review's 2020 40 under 40 guide. She is a member of Women in Cybersecurity and Girls Who Code. Ms. Kelly holds a Bachelor's degree from Wake Forest University and a Juris Doctorate from the University of Tennessee College of Law. Reach her at **jordan.kelly@fticonsulting.com** or **linkedin.com/in/jordanraekelly/**.

Endnotes

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
2. The number of ransomware attacks in the financial services industry carried out by Scattered Spider and countless other ransomware groups continues to rise. Numbering 64% increase in ransomware attacks across the industry in 2023. See **https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global/**
3. https://www.ibm.com/reports/data-breach?utm_content
4. https://fticybersecurity.com/2023-12/threat-intelligence-report-the-next-evolution-of-threat-actor-pressure-tactics/
5. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia
6. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
7. https://www.ibm.com/reports/data-breach
8. https://www.sec.gov/newsroom/press-releases/2023-139
9. https://www.sec.gov/news/press-release/2024-58
10. https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect
11. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311011
12. https://www.pillsburylaw.com/en/news-and-insights/cyber-incident-reporting-critical-infrastructure.html
13. https://ofac.treasury.gov/media/912981/download?inline
14. https://www.ibm.com/reports/data-breach?utm_content
15. https://fticybersecurity.com/2024-02/threat-intelligence-report-black-hat-generative-ai-tools/

ABA RESOURCES

Ransomware Toolkit
aba.com/ransomware

CSBS Ransomware Self-Assessment Tool
www.csbs.org/ransomware-self-assessment-tool

***ABA Banking Journal*: The realities of ransomware**
bankingjournal.aba.com/2022/04/the-realities-of-ransomware

***ABA Banking Journal*: The anatomy of a ransomware attack**
bankingjournal.aba.com/2023/05/the-anatomy-of-a-ransomware-attack