Resilience in Action – Lessons from the Field

Executive Summary

The Financial Services Information Sharing and Analysis Center (FS-ISAC), in collaboration with its members, government partners, and other stakeholders, coordinates information sharing and analysis during cyber incidents that affect the financial services sector and conducts exercises that test the sector's resilience to operationally disruptive events. After each incident and exercise, FS-ISAC undertakes a thorough analysis of the sector's response to identify best practices, recommend areas for improvement, and identify gaps in existing response capabilities.

This report covers notable incidents and exercises that occurred between January 2023 and March 2024, particularly incidents that affected trading, payment, and settling. In that period, a variety of cyber attacks disrupted key services in the financial sector, including attacks on a securities lending technology platform and a third-party provider of cleared derivatives services. FS-ISAC analysis of those incidents indicate resilience best practices including:

1. Business impact analyses
2. Refining business continuity plans
3. Tracking and communicating roles and responsibilities

This report provides an overview of that analysis in an anonymized and aggregated format that can be distributed widely.

1. Conduct a Business Impact Analysis

Identify adverse effects to the financial sector

Historically, firms conduct a business impact analysis (BIA) to determine which systems need to be available for business continuity. The process should be expanded to mission-essential functions that cannot tolerate downtime without creating adverse effects *across the financial sector*.

For example, a ransomware incident shut down operating systems used to clear trades in the primary US Treasury market in 2023. Such incidents can cause negative

cascading impacts across the sector. A BIA should determine how much downtime can occur before negative effects begin and considerations specific to incidents with potentially sector-wide impact.

For instance, it may be necessary to consult with experts throughout the sector, including government partners, as it was in this incident, to calculate how much downtime can occur before sector-wide impacts begin. It may also be necessary to disconnect from firms experiencing a cyber event to prevent further infection, but that decision can require critical service providers to quickly provide creative work-around solutions to keep business operations functioning. Such issues are crucial to effective responses to incidents targeting "no fail" operations, such as the trading of primary US Treasuries.

Inventory critical suppliers

Business functions and cybersecurity teams may not have equal knowledge of critical third-party suppliers until an attack occurs. Including those suppliers in the BIA can speed remediation.

For example, when a key player in a securities lending platform suddenly went dark due to a ransomware attack, traders were unable to see who they had made deals with, which made it difficult to properly allocate capital for those trades. The incident also revealed that several firms were relying on a single provider. Some security teams were not aware that their firm was using this platform until the business side indicated that something was amiss.

When assessing the criticality of a supplier for inclusion in a BIA, The Federal Financial Institutions Examination Council (FFIEC) recommends asking the following questions:[i]

- What is the nature of the customers and stakeholders? Are they corporate, interbank, retail, or non-bank financial services?
- What is the nature and extent of the activity – products, services, means of delivery, role? For example, payment and settlement systems?
- What impact would disruption of the function have on markets and infrastructure?

- Impact on other financial services firms and markets?
- Speed at which disruption would cause impact?

Incidents involving third parties or counterparties can help refine these questions and bring answers into sharper focus.

2. Track and Define Roles and Responsibilities

Identify key personnel on the business side

Cyber incidents impacting core business functions require an enterprise-wide response, particularly incidents affecting third parties – the business side is often the first to discover a disruption. Identifying and educating key personnel outside of cybersecurity to report disruptions is crucial to the security team's ability to maintain situational awareness quickly when incidents involve a third party.

Build communications channels between cyber and business

Multiple business units are involved in decision-making when an incident occurs, including the C-Suite, trading desks, lines of business, dedicated risk assessment professionals, as well as cyber and information security teams. Individuals and departments who normally do not interact will need to come together to provide continuity for the health of the firm. Determining the individuals who will establish clear lines of communication across the organization is essential. At the practical level, contact information will need to be collected and disseminated to all parties with multiple methods of communication included.

3. Refine Business Continuity Plans

Consider creating enterprise-wide working groups to consult with cyber responders

Financial sector companies are highly interconnected and interdependent. As a result, cybersecurity decisions – such as disconnecting from a third-party victim of a ransomware attack – can have significant business risk implications to the institution

and to the sector. Financial institutions should consider creating enterprise-wide working groups to consult with cyber responders.

Such cross-functional groups can provide insight that ensures cybersecurity response planning and incident response decisions are made in consideration of mission critical systems and infrastructure, within the company's stated risk appetite. In some cases, it may be prudent to accept more risk – such as using removable media or forgoing the full vendor risk assessment process to pivot quickly to a new provider – if the working group suggests that the business operation needs to be continued.

Understand your information technology stack and its dependencies

Many lines of business rely on automated systems, but security teams may not fully know the system's utility until it stops working. Firms should make every effort to identify the order management software and third-party vendors involved in trading desks and the vendor systems that process and manage financing transactions, such as securities lending and repurchase agreements.[ii]

Understand and practice backup capabilities for business-critical services

Ransomware incident responses commonly involve disconnecting from the victim and switching to manual processes to maintain operations. Firms should exercise converting to manual processes with their business units. When the securities lending platform mentioned above was attacked, its traders had to quickly move to manual trading. While the overall impact on the sector was low, it did raise the costs of those trades and interfered with the impacted firm's ability to capture regulatory reporting requirements. Employees should know how long it takes to move to fail-over systems, how to maintain manual operations at an acceptable level, and how to retrieve data from a system infected with malware and safely move it to a sterile environment.

Outlook

A sudden loss of service can cause severe operational consequences to the targeted institution, with cascading effects throughout the global financial sytem. Attacks on platforms involved in trading, payment clearing, or payment settling create immediate impact. Disruptions to capital markets and investment activities are similarly

consequential, as those functions are core to the financial sector's safety and soundness. A significant disruption or prolonged degradation of the sector's ability to carry out these functions can have economic and national security implications as well.

As we move into 2024, it is clear that the threat landscape is changing but not improving. As long as threat actors can profit from cyber attacks, the financial sector should expect disruptive impacts. As FS-ISAC's Navigating Cyber 2024: Annual Threat Review and Predictions report describes, ransomware attacks surged in 2023. Indeed, threat actors extorted over $1 billion USD from victim organizations,[iii] which also suffered the financial loss of productivity, reputation, and remediation.

This is why firms, as well as regulators, focus on operational resilience – and every incident, no matter how challenging, provides valuable insights into the effectiveness of business continuity plans. Firms that are ready for this inevitability by fostering a culture of resilience and communication will recover faster with less disruption. A solid business continuity plan coupled with a culture of transparency, creative problem-solving, and leveraging past incidents for learning is ideal.

---

[i]FFIEC Information Technology Examination Handbook: Business Continuity Management. https://ithandbook.ffiec.gov/media/2nifgh2b/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf TLP White.
[ii]FINRA. "Report Exam Findings and Observations for Business Continuity Planning." 2019. TLP WHITE Business Continuity Plans (BCPs) | FINRA.org
[iii]Chainalysis. "Ransomware Hits $1 Billion in 2023." TLP White. February 2024.

