sifma

Invested in America

Reconnection Framework

Guidelines for Remediating Cyber Events Impacting the Financial Ecosystem

November 2023

Contents

Introduction 4
Purpose 5
Principles 5
Governance and Communication 6
Reconnection Phases: Five-Step Mitigation Framework 6
Phase 1: Assess 8
Outcome 8
Technical Process 8
Pre-requisites 8
Phase 2: Remediate 9
Outcome 9
Technical Process and Sequencing 9
Pre-requisites 9
Phase 3: Assure 10
Outcome 10
Attestation 10
Validation 10
Communication 10
Pre-requisites 10
Phase 4: Reconnect 11
Reconnect Guidelines (i) 11
Reconnect Guidelines (ii) 12
Phase 5: Recover 13
Outcome 13
Technical Process 13
Pre-requisites 13
Appendix – Technical Steps and Recommendations to Consider 14
SIFMA Contacts 19

SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks, and asset managers whose one million employees provide access to the capital markets, raising over $2.9 trillion for businesses and municipalities in the U.S., serving clients with over $20 trillion in assets and managing more than $72 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

Introduction

In the financial industry today, there are several industry exercise programs – such as the U.S. Treasury's Hamilton Series, SIFMA's bi-annual Quantum Dawn and the Financial Services Sector Coordinating Council (FSSCC) Exercise Committee critical infrastructure protection initiatives – that explore how different types of cyber-attacks (for example, destructive malware, DDoS, ransomware, and so on) could impact the financial ecosystem. In addition, in jurisdictions around the world, similar cyber exercise programs exist tackling difficult cyber response and recovery issues. After-Action reports from these exercises pointed out the need for a "market re-entry" or reconnection protocol.

SIFMA was tasked with organizing a working group of subject matter experts to develop a reconnection protocol, which was subsequently "tested" during several industry exercises led by the Analysis and Resilience Center (ARC). Resulting from these efforts is the following Reconnection Framework: a voluntary series of steps, common practices, and activities a firm could take to assess, contain, remediate, and recover from a significant cyber event impacting the firm and its downstream trading partners – and to communicate, provide assurance, and facilitate reconnection with trading partners.

The steps outlined in this document are intended to provide recovery and reconnection guidance for a financial institution severely impacted by a cyber intrusion that requires the firm to shut down or disconnect compromised systems, data, operations or supporting technologies to contain the situation.

In some cases, a firm may decide to "disconnect". These cases include:

- **From the financial ecosystem**: to limit operational or technological impacts to upstream and downstream trading partners and/or critical third parties.
- **From the Internet**: to ensure that on-line transactions involving brokerage or banking clients are not compromised thereby limiting potential consumer harm.
- **During a period where the source of the incident is unknown as a cyber event**: This may first manifest itself by impacting operations, data, applications, or technology infrastructure. Firms will disconnect to provide Cyber Incident, Business Continuity, IT Incident and Crisis Management teams time to assess the situation and determine best remedial steps.

There are many issues a compromised firm must address to reconnect to the financial ecosystem after the malware has been contained and mitigated. Most importantly is how the firm should communicate, coordinate, and provide assurance to (what could be dozens of) trading partners in the most efficient and effective way to convey that the problem has been resolved and will not recur. This is crucial so the firm and its trading partners can resume normal business operations.

Purpose

This document provides best practice guidance to aid the process of resuming business and safely reconnecting an organization that has been technically quarantined after suffering a material cyber incident. The steps outlined in this framework will facilitate the safe recovery and restoration of services based upon an understanding of the root cause, assurance that the impacted systems are operating in a known trusted state, and the following of a controlled reconnection process. This Reconnection Framework is intended to support and inform a technical view on reconnection, as well as to inform broader resilience planning. A technical position may be factored alongside other business considerations when a more strategic decision on reconnection is required.[1]

This approach is considered good practice, and obtaining full assurance of system and data integrity may extend beyond business risk appetites. The levels of assurance required will vary by incident, depending on the compromised organization, the materiality of the impacts, sophistication of the attack, and so on. The relevant response groups should therefore use this framework to calibrate agreed specifics that need to be achieved against each outcome statement, ideally at the outset of each phase of activity.

Principles

No organization is immune to attack, and thus the following overarching imperatives apply to the reconnection protocol outlined within this document:

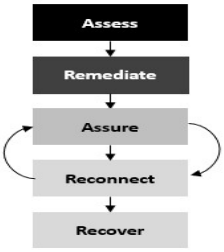
- All parties will engage in a non-judgemental fashion towards the compromised organization.
- All parties will assist the compromised organization to resume their business operations as fast as safely possible.
- There will be zero tolerance for anti-competitive behavior.
- The compromised organization should consider engaging independent expertise where appropriate, and openly provide evidence and assurance in support of technical considerations.
- To ensure full transparency throughout the process, all major decisions and actions will be recorded and openly communicated between key stakeholders, including: the compromised organization, reconnecting organizations, relevant sector response groups, law enforcement, and the regulators.

[1] *In the U.S., this is likely to be coordinated through the Securities Industry and Financial Markets Association (SIFMA) for systemic incidents.*

Governance and Communication

- Organizations should communicate regularly with relevant national cybersecurity agencies, sector response groups, customers and partners, regulators, law enforcement, and their supply chain throughout the incident.
- Progress through each of the phases of this framework should be communicated via the relevant sector group(s) coordinating the response.
- During the Assure phase, organizations should provide an attestation confirming the status of previous phases. This attestation should be signed by an individual accountable for security within the organization.

Reconnection Phases: Five-Step Mitigation Framework



Phase	Outcomes
Assess	The compromised organization has identified the type and extent of the attack and implemented its incident response playbooks. The compromised organization has sufficient understanding of (i) the attack to limit further impacts and (ii) impacts to operations, technology, markets, customers, and supply chain to facilitate remediation.
Remediate	The compromised organization has restored affected systems to a known trusted state that is appropriately protected and can evidence or demonstrate the integrity of remediated systems, their software images, libraries, reference data, hardware and other components as required.
Assure	The compromised organization has provided an attestation to external stakeholders, signed by an individual accountable for security within that organization, to provide sufficient assurance that it is ready to be reconnected and to resume normal operations. The attestation will provide the detail for firms to make a reconnection Go or No-Go decision.
Reconnect	(i) The compromised organization has reconnected to selected external stakeholders and undertaken test transactions to confirm that data/system integrity has been re-established. (ii) Following confirmation of the Reconnect (i) phase, the compromised organization has conducted additional reconnection and begun ramping up activity under heightened monitoring to normal levels.
Recover	The compromised organization has fully recovered and restored affected services. A plan has been coordinated with external stakeholders for the phased standing down of incident response processes and engagement to return to normal operations/Business as Usual (BAU).

Financial firms can use the steps above to advise trading partners as to what actions have been taken to remediate the issue and to provide the firm's readiness to recover and reconnect.

The five-step mitigation framework has two main purposes:

- To outline best or common practices financial firms use to recover from cyber events and resources relied upon to complete each step.
- To provide the industry with a structured way to facilitate efficient and effective communications to potentially reduce time to recover.

For example, a compromised firm, when having a reconnect discussion with trading partners, may simply assert that they have followed the guidance and are ready to reconnect and resume normal business operations.

The following pages outline detailed steps impacted firms could take during each Phase of the reconnection process.

Phase 1: Assess

Outcome

The compromised organization has identified the type and extent of the attack and implemented its incidence response playbooks. The compromised organization has sufficient understanding of (i) the attack to limit further impacts and (ii) impacts to operations, technology, markets, customers, and supply chain to facilitate remediation.

Technical Process

Complete comprehensive assessment of impacts to:

- Operations (lines of business/geographic scope/services provided to industry).
- Technology (infrastructure/applications/cloud hosted services).
- Data and Privacy (market/reference/customer Personal Identifying Information (PII).
- Transactions (volume/type/recoverability).
- Customers (number/geographic spread).
- Trading Partners/ecosystem (Impacted firms list/critical infrastructure/third parties/Financial Market Infrastructure (FMIs).
- Liquidity/Payment System Affected (impacted payment systems/volume of cleared/settled transactions/trapped liquidity financials).

Pre-requisites

Organizations should:

- Have business-wide incident management procedures to quickly coordinate assessments during an incident.
- Consider having contractual arrangements in place with an appropriate cyber incident response company.
- Have an understanding of any incident reporting regimes related to the impacted service.

Phase 2: Remediate

Outcome

The compromised organization has restored affected systems to a known trusted state that is appropriately protected and can evidence or demonstrate the integrity of remediated systems, their software images, libraries, reference data, hardware and other components as required.

Technical Process and Sequencing

- Where possible, secure and preserve appropriate information for future investigative analysis and legal use, such as indicators of compromise (IoCs), logs, images, and other forensic evidence.
- Industry best practice protections are deployed, tested and in place to minimize a recurrence of the compromise, prior to commencement of the restoration of systems and services.
- Undertake integrity checks to verify all components are ready to restore.
- Validate that no other changes, incidents, or events are occurring that could impact the restoration process.
- Following an internal Go/No-Go decision within the compromised organization, all parties involved in the process; including assurance functions, execute the remediation plan conducting pre-agreed checks at each stage.
- Ensure all impacted and relevant systems and applications are appropriately patched and hardened.
- Perform assurance and integrity tests on the services, applications, systems, and network to validate and certify all systems as operational and functioning normally.
- Maintain heightened monitoring for an appropriate period to ensure that no abnormal system, user, or network behavior is observed.

Pre-requisites

Organizations should:

- Develop an inventory of trusted sources and back-ups for each of the systems to be remediated. This should remove potential obstacles to re-creating a trusted environment and develop safeguards to reduce the risks to the remediation process.
- Have an overarching test plan to validate integrity at every stage of the process.

Phase 3: Assure

Outcome

The compromised firm has provided an attestation to external stakeholders – signed by an individual accountable for security within that organization – to provide sufficient assurance that it is ready to be reconnected and to resume normal operations. The attestation will provide the details for firms to make a Go or No-Go decision.

Attestation

Attestation should include:

- Timeline of attack including method and initial infection vector.
- Impact to services, data, endpoints, servers, supply chain, and so on.
- Remediation activity – including detail on steps taken in the first two phases of the framework.
- Any aspects that have not been completed should be called out explicitly.
- Where possible, timeline of next steps including planned enhancements to security posture.
- Where possible, evidence of cyber incident response activities undertaken should be provided.
- Compromise assessment summary outcome report (e.g., incident review report).

Validation

- Validate data transfer with key stakeholders.
- Validate integrity of any software code.

Communication

- Organizations should leverage relevant sector response groups to enable faster and more effective communication with the sector.
- The compromised organization should leverage an appropriate incident response company as part of their assurance activity to external stakeholders.

Pre-requisites

- Organizations reconnecting to the compromised organization should be prepared to review any IOCs, TTPs received from the compromised organization as part of their own assurance activities.
- Organizations should consider developing and rehearsing an internal assurance and attestation framework to support efficiency throughout this phase.

Phase 4: Reconnect

There are two sets of Reconnect Guidelines:

i. For reconnecting to selected external stakeholders and testing transactions to confirm that data/system integrity has been re-established.
ii. And, following confirmation of Reconnect (i), for conducting additional reconnection and ramping up activity under heightened monitoring to normal levels.

Reconnect Guidelines (i)

Outcome

The compromised organization has reconnected to selected external stakeholders and undertaken test transactions to confirm that data/system integrity has been re-established.

Technical Process

- Establish connectivity with selected stakeholders, agree on process for a test exchange of data and validate that these data exchanges are as expected.
- Make low-value test transactions with key stakeholders. This should include 'two-way' and 'end-to-end' transactions. Where relevant, compromised organization to define a strategy to validate connectivity and data integrity. These tests should ideally be conducted first in the test system, then out-of-hours in the production system. Organizations may decide to conduct them in-hours depending on sector urgency to establish reconnection.
- Undertake heightened transaction monitoring across all relevant organizations for an agreed period.
- Results during this phase should inform active updates to key stakeholders as to the continued accuracy of attestation provided during the Assure phase.

Pre-requisites

- IOCs/TTPs involved in the attack should be explicitly shared with all those being reconnected to, so they can assure selves as well detection wise prior to and following.
- Organizations should ensure they have prepared protocols for each type of managed system reconnection they may need to undertake, to include:
    - Types of messages to be exchanged, and with which other critical stakeholders.
    - Success criteria for those exchanges to demonstrate data/system integrity.

- Mitigation process for an unsuccessfully managed reconnection (e.g., to what phase the wider reconnection process should be rolled back), both internally and with sector peers.
- Organizations should regularly exercise and rehearse each type of system reconnection protocol to ensure streamlining and sufficiency.

Reconnect Guidelines (ii)

Outcome

Following confirmation of Reconnect (i), the compromised organization has conducted additional reconnection and begun ramping up activity under heightened monitoring to normal levels.

Technical Process

- Full connectivity with key stakeholders should be re-established using a phased approach, where relevant.
- Transaction/activity testing should be considered prior to reconnection with each partner, where relevant.
- Heightened monitoring and enhanced support across all relevant organizations should continue for an agreed period of time.

Pre-requisites

- Organizations should have protocols in place establishing the criticality of key partners (for example, if reconnection needs to be phased, which partners will be prioritized).
- Organization should have defined, internally approved protocols in place to authorize the full reconnection of services.
- Appropriate test and roll-back plans should be prepared and approved prior to reconnection attempts/activities.
- Full reconnect and restore activities should be included and tested on a regular basis as part of an organization's incident response plan.

Phase 5: Recover

Outcome

The compromised organization has fully recovered and restored affected services. A plan has been coordinated with external stakeholders for the phased standing down of incident response processes and engagement to return to normal operations/Business as Usual (BAU).

Technical Process

- Service is restored following successful results from the Reconnect phase.
- Heightened transaction monitoring across all organizations stops and monitoring activities return to BAU.
- Specialist support remains assembled for an agreed upon period in case of additional issues.
- Communications are issued to internal and external parties, particularly any interested parties who have experienced downstream impacts.

Pre-requisites

- Organization should have defined, internally approved protocols in place to authorize the full restoration of services.
- Full reconnection and restoration activities should be included and tested on a regular basis as part of an organization’s incident response plan.
- A post incident review process is established to evaluate root cause analysis of the incident, and all response mechanisms.

Appendix – Technical Steps and Recommendations to Consider

This Appendix builds on the above guidance and provides more detailed technical recommendations to aid the process of resuming business and safely reconnecting an organization that has been technically quarantined after suffering a material cyber incident. Organizations can refer to this Appendix when building their own reconnection protocols.

The recommendations on pages 15-? are best practices. There is no “one-size-fits-all” approach to incident response and coordination as all incidents are different and require their own flexible response. Based on the event, some services may be ready before others. The process may not necessarily share the same linear flow of phases as what is illustrated below.

Through each phase, stakeholders across Crisis management (CxOS, Legal, Compliance, Operations, Payments, Communications) Incident Management (InfoSec, IT, BCP), and Cyber Intel will be involved in supporting reconnection efforts for their compromised firm.”

Phase 1: Assess
Identify Impact Specifics

Operations Impacted?

- Lines of business?
- Business processes?
- Geographic scope
- Services provided to industry

Technologies Affected?

- Applications (in house or third-party)
- Data Network (internal/external)
- Voice communications
- Cloud SaaS
- Other

Clients/Customers Affected?

- Number, %, and type of clients
- Geographic spread

Data Compromised?

- Market
- Reference
- Customer/employee PII, PHI
- Regulatory Notification required?
- Privacy obligations (e.g., GDPR)
- Confidentiality, Integrity, Availability (CIA) Impact
    - Corrupt data replicated?
    - Backup data corrupted?
    - Data exfiltrated?

Transactions Affected?

- Volume
- Type(s)
- Market Instruments
- Recoverable?
- Lost?
- Cancellable by Regulators?

Trading Partners/Ecosystem Impacted?

- Number of impacted firms? (Impacted firm list)
- FMUs/FMIs?
- SIFIs/GSIFIs?
- Exchanges?
- Third-Parties?
- Critical Infrastructure? (notify responsible government agency)

Liquidity/Payments Systems/Disbursements Affected?
• Impacted payment systems • Trapped liquidity financials • Volume of cleared/settled transactions • Disbursements made

Phase 2: Remediate

Remediate Immediate Cyber Impact

• Identify tools and resources required to remediate impact
• Take all affected systems off-line
• Eliminate malware and actor from all environments
• Enable BCP/DR Plans:
  − Recovery to backup/DR systems?
  − Processes shifted to other locations?

Remediate Security Control Failures/Enable Monitoring
• Patch relevant remaining systems minimize chance of reoccurrence • Implement compensating controls where appropriate • Implement “circuit breakers” to prevent further impacts • Enable enhanced monitoring to detect where issue may occur elsewhere in the architecture
Remediate Incident Impact

• Validate all systems and data sources are clean (live, backups)
• Operations identifies corrupt transactions are in touch with trading partners and where necessary:
  − Secure agreements from Regulators to roll back certain transactions which are significantly “out of market”
  − Secure agreements for FRB to provide funding from discount window

Prepare for Resumption
• Ensure backup systems / applications up and running and data is restored

Phase 3: Assure

Provide Assurance to Impacted Firms

- Convene face-to-face meeting, if appropriate, or teleconference with impacted firms.
- Send relevant information to impacted firms.
- Compromised organization provides "attestation," indemnification, or assurance from CXO (or similar) to trading partners/impacted firms that all material remediation efforts are complete, and the firm is, to the best of their knowledge, ready to resume normal operations.
- Includes assurance that threat actor has been removed from affected networks and describes impacts to affected entity.
- Include information on any issues the firm has not completely recovered from.
- Confirm firm's financial health.
- Validate integrity of software delivered before, during and after incident.
- Validate integrity of files exchanged.
- Officially notify appropriate Regulatory and law enforcement bodies as needed.
- When relevant Issue media response from corporate communications and sector, where necessary, regarding timeline to reactivation and incident.

Re-establish Connections

- Establish connectivity with key utilities and trading partners, using updated credentials as required.
- Exchange handshakes.
- Validate data exchanges are normal.
- Check for data integrity issues (software, files, and business transactions).

Phase 4: Reconnect (I) and (ii)

Reconcile

- Reconcile corrupt transactions/confirm mismatches on existing, pending and completed transactions.
- Identify and ring-fence all pending/inflight/future dated transactions.
- Identify and resolve extant liquidity concern.
- Conduct final clearance/settlement activities.

Execute Test Transactions

- Agree on test transaction types and symbols:
  - Use low value test transactions
  - Use current dates (no future transactions)
  - Use "two-way" and "end-to-end" transactions i.e., "receive and send"
- Test data file transfer, software/code as required by the incident and relationships with key stakeholders.
- Send test transactions to utilities and trading partners from test environment.
- Conduct simple ping, transaction, and data integrity tests off-hours and in production.
- Implement heightened transaction monitoring across all affected institutions.
- Validate test transactions are handled normally.

Validate Test Transaction Results
• Hold “industry discussions where compromised organization and impacted firms discuss test transaction results.
Gradually Escalate Activity

• Send live transactions over the course of 1-3 business days, e.g.:
  − Wave one: send 25% of normal traffic load – cash transactions only
  − Wave two: send 50% of normal traffic load – cash transactions only
  − Wave three: send 100% of normal traffic load – cash and futures transactions
• And/or set dollar value thresholds e.g., no transactions with dollar value > x million.
• And/or initially limit full connections to a “friendly” single utility or trading partner.
• Validate transactions are handled normally.

Phase 5: Recover

Return to Business As Usual (BAU)
• Remove debit/credit blocks on client accounts. • Reset circuit breakers. • Continue to monitor activity over the next several days: − Hold daily industry touch point conference calls before the open, at mid-day and after market close.
Conduct industry and individual firm *After Action Reviews* and review security control uplifts implementation.

SIFMA Contacts

This is a reference document that organizations can use when building their own reconnection protocols. If you have further questions, please contact Tom Price and Tom Wagner at 212.313.1000:

Tom Price
Managing Director, Technology, Operations, and Business Continuity
SIFMA

Tom Wagner
Managing Director, Financial Services Operations
SIFMA