TLP CLEAR

G7 Cyber Expert Group: Reconnection Framework Best Practice

Technical Annex

Introduction

Reconnection is the process of restoring technical access and integration to an organisation that has been technically quarantined after suffering a material cyber incident. This includes a phased resumption of business operations, beginning with the technical reconnection of stakeholders and entities to the organisation.

This is a supplementary annex to *G7 CEG Reconnection Framework Best Practice* (2025). Like the main paper, this annex does not set guidance or regulatory expectations. Its aim is to identify effective practices and approaches that jurisdictions and their institutions may utilize to implement reconnection frameworks in the event of a cyber incident and explores the preliminary considerations and technical processes that may support compromised organisations in their reconnection efforts following a cyber incident[1]. The document also introduces the concept of disconnection.

'G7 CEG Reconnection Framework Best Practice' drew on the insights and experiences of public-private partnerships across G7 jurisdictions. This technical annex to the main document particularly draws on work by the UK Cross-Market Operational Resilience Group (CMORG), and joint work from the US Financial Services Sector Coordinating Council (FSSCC) and US Securities Industry and Financial Markets Association (SIFMA). Our thanks to those authors.

Overview

This annex is set out in five sections: Phase 0, 'Disconnection'; phase 1, 'Assess'; phase 2, 'Remediate'; phase 3, 'Assure'; phase 4, 'Reconnect'; phase 5, 'Recover'. Each section provides additional detail, including the anticipated outcome for compromised organisations, preliminary considerations for each phase, and technical processes a compromised organisation may consider undertaking as part of each phase. It is important to note that, while articulated here as phases, these activities often run in parallel and may not be seen as strictly linear.

The document also includes a Frequently Asked Questions (FAQ) appendix to assist compromised organisations in developing an attestation to client organisations, regarding the status of their actions to contain and remediate the incident that led to disconnection.

Phase 0: Disconnection

[1] The term 'organisation' here encompasses firms, authorities, and third parties. Though this document is intended primarily for financial sector organisations, it can be leveraged by third parties.

A pre-cursor and useful context to reconnection is disconnection; client organisations may decide to 'disconnect' from a compromised organisation, or vice versa.

Anticipated Outcomes

The compromised organisation is disconnected from the client organisation(s).

Preliminary Considerations

Client organisations may consider having business-wide disconnection procedures in place to enable effective and targeted disconnection during an incident.

There are several reasons a client organisation may or may not choose to disconnect from the compromised organisation, including:

- Intelligence suggesting the threat actor has not been removed from the compromised organisation's network and that there is potential for further disruption or contagion.
- When continuing to send sensitive information to the compromised organisation could result in a breach of that data.
- When continuing to send data, especially transaction data, may complicate reconciliation and/or result in uncertain positions.
- While fear of contagion could also lead to a disconnection decision, it is recognized that many organisations have made significant investments in compensating controls and monitoring capabilities that significantly reduce this risk. These may be considered in relation to the specifics of a given scenario to support optionality for decision-makers.
- Other risks and considerations might emerge, such as reputational risks associated with the event.

Disconnection Technical Process

Firms could consider the following factors when deciding to disconnect:

- Type of security incident and whether it is malicious or non-malicious (e.g., malware, ransomware, business email compromise, insider threat, compromised website).
- Level of impact of the security incident to the compromised organisation.
- Current status of the security incident (i.e. remediated, not contained, unknown).
- Level of cooperation from the compromised organisation.

Client organisations may have more than one connection with a compromised organisation e.g. multiple transactional connections, domain level connections (e.g. email), and so forth. Disconnecting does not necessarily mean complete termination of all connections between the two parties, since different connections might present different levels of risk. Organisations should assess whether physical or logical disconnection is required. Organisations may have electronic access agreements in place with businesses

that require connections to provide services. They should be considered before disconnection.

Other examples include:

- Suspend connection – remain physically connected but switch off the systems which exchange data with the compromised organisation. This could be conducted at the compromised organisation, the client organisation, or both.
- Suspend connection access – remain physically connected but remove or prevent the compromised organisation from accessing systems which exchange data, but which remain accessible to others, e.g. FMIs' service platforms. This may also include removing the access rights of the client organisation to access data and systems.
- Pause traffic – remain physically connected and maintain access rights but agree to stop sending traffic e.g. stop submitting transactions or stopping emails. This can include pausing only incoming or outgoing traffic, or both.

Business Risks vs. Technical and Cybersecurity Risks of Reconnecting

- The Framework focuses on the technical and cybersecurity elements of reconnection. However, reconnection inherently involves business considerations as well.
- The role of the cybersecurity function in the client organisation is typically to assess the residual cybersecurity risk based on information gathered from the compromised organisation and the client organisation's own threat intelligence.
- The role of the accountable business is to assess business market and sector considerations impacts and ultimately make the decision on whether to disconnect from or reconnect to a compromised organisation. While in urgent scenarios the cybersecurity function of the client organisation may initiate a disconnect, the decision to reconnect or not would typically remain with the accountable business within the client organisation, taking into account the cyber risk as articulated by the client organisation's cybersecurity function.

Phase 1: Assess

Anticipated Outcomes

- The compromised organisation has identified the type and extent of the attack and implemented its incident response playbooks.
- The compromised organisation has sufficient understanding of (i) the attack to limit further impacts and (ii) impacts to operations, technology, markets, customers, staff and supply chain to facilitate remediation.
- Following customer identification, the compromised organisation has established communications with impacted client organisations.

Preliminary Considerations

- Compromised organisations may utilise business-wide incident management procedures to quickly coordinate assessments during an incident.
- Compromised organisations may have contractual arrangements in place with an appropriate cyber incident response company.
- Compromised organisations should take steps to understand any incident reporting regimes related to the impacted service.
- Compromised organisations should be prepared to establish initial communications strategy towards the different stakeholders and especially with impacted client organisations.
- Where appropriate, compromised organisations may engage with relevant security agencies.

Assessment Technical Process

When available and appropriate the compromised organisation may seek the technical support of their national cyber security agency.

The minimum information a compromised organisation may want to provide to clients and other concerned stakeholders may include:

Information	Description
Timing of incident	The time that the incident occurred or other relevant timeline information.
Type of incident	The type of incident that has occurred, i.e. virus, DDoS, ransomware, malicious attack, phishing, etc.
Nature of incident	A concise description of the identified incident and its potential impact to clients (as detailed as possible).

	If data has been leaked or exfiltrated, provide an indication of the extent of the data exposure and classification of data.
Source of information	How the breach was discovered, i.e. through notification from another party, from self-discovery, etc.
Investigation details	What actions have been taken as part of investigating the incident to confirm its potential scope and impact, including identifying the tactics, technique and procedures (TTP) of initial infection: • Tactics (high level strategies of an attack) – reconnaissance, delivery, exploitation, espionage, insider threat • Technique (specific methods used to achieve tactics) – ransomware, phishing, brute-force attacks, SQL injection • Procedures (detailed steps taken) – execution of the techniques above
Remediation activities	Which actions have been taken, including: what has been done to mitigate/remediate the incident; whether a third-party cyber assurance company has been engaged; whether legal authorities are informed; whether there is regulatory impact; etc, in accordance with applicable regulatory requirements and protocols. (See 'Phase 3: Assure' for more examples)
Impact analysis	The impact to client organisation(s), including: • Operations – lines of business, business processes, geographic scope, services provided to industry; • Technology – infrastructure, applications (in house or third-party), data network, voice communications, cloud hosted services; • Data and Privacy – market or reference data, customer Personal Identifying Information (PII), Confidentiality, Integrity, Availability (CIA) impact (including corruption of data, backup data corruption, and data exfiltration).
Data-sharing	If available, share audit logs, Indicators of Compromise (IOC), and/or forensic reports.
Next steps	This may include what actions remain for completion, along with a full timeline for remediation and wider service restoration.

Phase 2: Remediate

Anticipated Outcomes

- The compromised organisation has restored affected networks 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.
- The compromised organisation has communicated these developments through ongoing engagement with impacted client organisations.

Preliminary Considerations

Compromised organisations may wish to:

- Develop an inventory of trusted sources and back-ups for each of the systems to be remediated. This could remove potential obstacles to re-creating a trusted environment and develop safeguards to reduce the risks to the remediation process.
- Have an overarching plan for detailed testing to validate integrity at every stage of the process.
- Where possible, secure and preserve appropriate information for future investigative analysis and legal use, such as indicators of compromise (IoCs), for example privileged account irregularities, unusual outbound traffic, or geographic irregularities, as well as logs, images, and other forensic evidence.
- Collaborate with impacted client organisations on any business workarounds in place to reduce impact of the disruption.

Remediation Technical Process and Sequencing

Remediation efforts will vary based on the specific situation of the incident. However, compromised organisations may take into account the following considerations:

<u>Remediate immediate cyber impact</u>:

- Take all affected systems off-line.
- Identify tools and resources required to remediate impact.
- Eliminate malware and actor from all environments.
- Enable business continuity plans.
- Recover to backup systems, if available.
- Potentially shift processes to other locations.

Remediate security control failures and enable monitoring:

- Industry best practice protections are deployed, tested and in place to minimise a recurrence of the compromise, prior to commencement of the restoration of systems and services.
- Where appropriate, patch relevant remaining systems, to minimise chance of recurrence.
- Implement compensating controls where appropriate.
- Isolate environments as necessary to prevent further impacts.
- Enable enhanced monitoring to detect whether issue might occur elsewhere in the network.
- Remediate remaining incident impact:
- Undertake integrity checks to verify all components are ready to restore, including all systems and data sources (live, back-ups).
- Operations team identifies corrupt transactions and contacts trading partners and/or other stakeholders where necessary.
- Validate that no other changes, incidents or events are occurring that could impact the restoration process.

Phase 3: Assure

Anticipated Outcomes

The compromised organisation has provided assurance to external stakeholders over the course of the incident culminating with an attestation, signed by an individual accountable for security within that organisation, to provide sufficient assurance that it is ready to be reconnected and to resume normal operations.

Preliminary Considerations

IOCs/TTPs involved in the attack may have been explicitly shared with all impacted client organisations.

Assurance Technical Process

- The compromised organisation may consider leveraging an appropriate incident response company as part of their assurance activity to external stakeholders.
- The compromised organisation may provide an attestation to client organisations regarding the status of their actions to contain, remediate and identify security uplifts based on incident analysis derived from the root cause analysis of the incident and infection vector.
- The attestation may include (but is not limited to, nor is this an exhaustive list):[2]That the compromised organisation is, to the best of their knowledge, ready to resume normal operations or even a still degraded but safe state of operations. This may be evidenced by steps taken in the first two phases of the framework, including assurance that threat actor has been removed, containment has been successful, and key systems and datastores are recovered to pre-infection resilience;
- That assurance and integrity tests have been performed on the services, applications, systems, back-up systems and network to validate and certify all systems as operational and functioning normally;
- Compromise assessment summary outcome report (e.g., incident review report), including information on any issues the firm has not completely recovered from – any aspects that have not been completed may be called out explicitly; and
- Outline of lessons learned, and planned enhancements made to prevent similar incidents in the future.
- Opportunity for client organisations' procedures to include effective challenge on compromised organisations' attestation activities to meet reconnection requirements.
- The compromised organisation may validate data transfer with key client organisations and validate integrity of any software code.

[2] See FAQs for considerations when developing an attestation.

- Opportunity for client organisations' procedures to include effective challenge on compromised organisations' attestation activities to meet reconnection requirements.

In addition to engaging bilaterally with client organisations, compromised organisations may leverage relevant sector response groups to enable communication of assurance with the sector.

Phase 4: Reconnect

The 'reconnect' phase has two key elements:

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

Phase 4i: Reconnection Guidelines

Anticipated Outcomes

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

Preliminary Considerations

Client and compromised organisations may consider preparing protocols for each type of managed system disconnection and reconnection they may need to undertake, possibly including:

- 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 may be rolled back), both internally and with sector peers.

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.

- Reconcile data, transactions and settlement:
- Reconcile corrupt transactions and 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 and settlement activities.

Make low-value test transactions with key stakeholders:

- Tests should replicate the range and behaviour of data expected in business-as-usual and may test the end-to-end process.[3] It is also recommended to use low

[3] Where data is exchanged two-ways, the test should replicate that.

value test transactions, to use current dates (no future transactions) and to test data file transfer, software and code as required by the incident and relationships with key stakeholders.

- Where relevant, compromised organisation to define a strategy to validate connectivity and data integrity.
- These tests may ideally be conducted first in the test system, then out-of-hours in the production system.
- Undertake heightened transaction monitoring across all relevant organisations for an agreed period.

Phase 4ii: Reconnection Guidelines

Anticipated Outcomes

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

Preliminary Considerations

- Compromised organisations should have protocols in place establishing the criticality of key partners (for example, if reconnection needs to be phased, which partners will be prioritised).
- Appropriate test and roll-back plans may be prepared and approved prior to reconnection attempts/activities.
- Organisations may consider testing full reconnect and restore activities on a regular basis as part of an organisation's incident response plan.

Technical Process

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

Phase 5: Recovery

Though not necessarily specific to the technical elements of the reconnection process, business resumption and recovery could be occurring while the reconnection process is taking place.

Anticipated Outcomes

The compromised organisation has fully recovered and restored affected services, and business / service levels reach an effective resilience position.

Preliminary Considerations

Full reconnection and restoration activities may be included and tested on a regular basis as part of an organisation's incident response plan.

Recovery Technical Process

- Service is restored following successful results from the 'Reconnect' phase.
- Client organisations have removed remaining barriers to the compromised organisation.
- Isolation mechanisms are reset.
- Communications are issued to internal and external parties, particularly any interested parties who have experienced downstream impacts.

See overleaf for Frequently Asked Questions (FAQ) appendix

Appendix: FAQs to consider when developing the attestation

What does an internationally recognised cyber incident response provider look like?

Internationally recognised cyber incident response providers can be vetted effectively by considering multiple factors. Personnel should hold relevant cybersecurity qualifications that are aligned with international standards and have a proven track record in resolving incidents.

Compromised organisations may verify that the cyber incident response provider has documented processes for detecting, containing, and recovering from incidents.

The compromised organisation may consider whether the cyber incident response provider has experience responding to incidents where the firm has experienced disconnection by their third parties. A cyber incident response provider may have the ability to communicate effectively with the compromised organisation's third parties and to produce detailed attestations and forensic reports to facilitate the assurance process of reconnection.

If the compromised organisation has cybersecurity insurance, the insurer will likely provide a list of pre-vetted cyber incident response providers.

Organisations providing services to regulated firms may consider maintaining a relationship with multiple cyber incident response providers to mitigate the risk that one cyber incident response provider does not have the resources available to support their incident or the scenario in which confidence in the cyber incident response provider is lost by the compromised organisation or its clients.

Organisations may also consider seeking contract terms with their cyber incident response provider that specify the requirements necessary to satisfy the assurance expectations set out in this framework.

What is the best way to share the attestation and forensic reports?

The compromised organisation should communicate on an ongoing basis with the disconnected firms. Through this communication, channels may be established to the relevant team(s) within the disconnected firms. These channels may be utilised for sharing the final attestation and forensic reports.

Where the compromised organisation does not have a direct line of communication to the disconnected firm, it may consider utilising the appropriate industry bodies to disseminate information regarding assurance activities, up to and including the attestation and forensic report.

Failure to communicate or provide the attestation and/or forensic reports directly to the disconnected firm(s) may delay the reconnection process.

How can I engage with relevant sector response groups?

Compromised organisations may consider utilising financial sector industry groups to share information related to the breach, as well as activities undertaken to assess and remediate the incident, in accordance with Phases 1 and 2 of the Reconnection Framework.

The compromised organisation may consider sharing assurance details and final attestation documentation with sector groups.

This information sharing may take the form of participating in crisis calls or providing written communications to those groups for circulation to its members.

However, the compromised organisation may not view communication to industry groups as a substitute for bilateral communication to disconnected firm(s).

Many disconnected firms will require bilateral live conversations with the compromised organisation before any reconnection decision is made. For these disconnected firms, the industry group calls serve to provide a baseline rather than the full assurance picture they require.

The compromised organisation may consult National Institute of Standards and Technology (NIST) guidelines for the secure sharing of sensitive information, such as Indicators of Compromise.

When should the attestation be ready?

The formal signed attestation is typically the final step in the assurance phase. For some disconnected firms, it may serve as a formality following extensive bilateral communication, while for others, it may be the basis for a reconnection decision. The scenario, as well as the individual firm's risk appetite, will dictate whether a client organisation/firm chooses to reconnect to a compromised organisation before an attestation is received.

Significant communication regarding the status of remediation activities is expected to occur between the compromised organisation and disconnected firm(s) before the final attestation is shared.

While the specific timeline for the final attestation will depend on the scenario, the compromised organisation may communicate with disconnected firms through established channels to clarify when they expect the final attestation to be available. This timeline estimate may evolve over the course of remediation activities.

Proactive and timely information-sharing by the compromised organisation is likely to reduce the total time required to reach a reconnection decision.

When should the forensics report be available?

The forensics report is typically the result of a more extended process and is not available during the assurance phase.

Disconnected firms may consider making a reconnection decision before the forensics report is available. For most firms, the forensics report is not deemed necessary to make that decision.

What is the difference between an attestation and forensics report?

An attestation is a record of the assurance steps a compromised firm has undertaken to identify, contain and remediate security enhancements based on the root cause analysis of the incident and infection vector.

The forensic report is a third-party created or attested report that outlines every aspect of Containment, Remediation, Restoration, Immediate Security Uplifts and Future Security Uplift Roadmaps.

Who may sign the attestation?

The attestation may be signed by an individual accountable for security or operations within the compromised organisation. This individual may possess the technical proficiency to discuss in detail all information included in the attestation.

The signer may have appropriate levels of seniority, familiarity with the products and be reputable and well-known to the disconnected firms.

The compromised organisation may consider in advance who would sign an attestation, depending on a range of scenarios, how that decision will be made, and whether multiple accountable individuals from different responsible functions would sign.

Have you provided the IOCs or other intelligence to the customer base?

The compromised organisation may provide Indicators of Compromise (IoCs), where possible, in line with Phase 2 of the Framework. Other intelligence such as TPPs may be considered for sharing.

The compromised organisation may consider in advance its process for sharing such information, including familiarity with NIST or other relevant guidelines for the sharing of sensitive information.

The compromised organisation may share IoCs before the final attestation to facilitate the reconnection decision. The attestation may confirm that IoCs have been shared.