Cyber Security Guidance Paper – Responding to a Cyber-attack on a Securities Services Participant

July 2020

Disclaimer

It is ISSA's intention that this report should be updated periodically. This document does not represent professional or legal advice and will be subject to changes in regulation, interpretation, or practice.

None of the products, services, practices or standards referenced or set out in this report are intended to be prescriptive for Market Participants. Therefore, they should not be viewed as express or implied required market practice. Instead they are meant to be informative reference points which may help Market Participants manage the challenges in today's securities services environment.

Neither ISSA nor the members of ISSA's Working Group listed in Appendix 5 warrant the accuracy or completeness of the information or analysis contained in this report.

Contact

International Securities Services Association ISSA
c/o SIX Group Services
Hardturmstrasse 201
P.O. Box
CH-8021 Zurich, Switzerland

Contact +41 58 399 3051
issa@issanet.org

Abstract

Cyber-attacks continue to increase in frequency, sophistication and impact. These attacks have the potential to disrupt critical financial services and could undermine the security and confidence of the financial system. In the 2020 Allianz Risk Barometer, the threat to businesses around the globe posed by cyber incidents moved to become the number one threat.

This document provides guidance for the incident management processes of Securities Services participants and utilizes the most impactful scenarios identified in the 2018 ISSA paper, ***Cyber Risk Management in Securities Services***[1], to develop Considerations that may enhance the playbooks used by securities servicers during a material cyber event. More specifically, this document is based on two scenarios. In the first scenario, a CSD is compromised by a material operational event. In the second, the material operational event occurs at a large Custodian. For these scenarios, this paper proposes Considerations for both the compromised CSD or compromised Custodian and other non-compromised organizations in the Securities Servicers value chain. The Working Group believes that these Considerations are applicable to any disruption, regardless of the cause of the service interruption.

These actions are not exhaustive and should be based on the size, type and complexity of business operations; customers and counterparties; products and markets traded; and market interconnectedness.

Market Participants should have their own cyber playbooks focused on their own recovery actions from a cyber incident. This guidance is therefore designed to provide supplemental information on what the Securities Services market segment believes needs to be added, where appropriate, to a firm's internal playbook to cover a material operational event which comprises a CSD or Custodian on which the firm relies.

Target Audience

This document is targeted at Executive Management, Business Operations, Business Continuity and Disaster Recovery specialists, Information Security Professionals and Risk Managers working within the Securities Services industry. It is aimed particularly at those working within Central Securities Depositories, Global and Sub Custodians and Securities Market Infrastructure and Utility firms.

Acknowledgements

This paper is the result of efforts by a team of experts drawn from the ISSA Operating Committee members and other ISSA participating member firms. All participants have supplied invaluable market information and input into this document. The names of participating firms and the individual contributors are listed in Appendix 5. The ISSA Executive Board wishes to thank all supporters for their contributions, as well as to their firms who have enabled their participation.

[1] ISSA, Cyber Security Risk Management in Securities Services available at: https://www.issanet.org/e/pdf/2018-10_ISSA_Cyber_Risk_in_Securities_Services.pdf

Table of Contents

1. Executive Summary

This paper builds on the work done in the ISSA report **Cyber Security Risk Management in Securities Services** from October 2018. The first sentence of that report is still extremely pertinent: «Significantly adverse consequences associated with cyber-attacks are seen on a far too regular basis across many industries, services and infrastructure environments. » The responses to the COVID-19 pandemic, with extensive working from home, have introduced more avenues for cyber-attacks.

The Susceptibility Factors and Risk Clusters described in that document continue to be valid and will not be repeated here. ISSA's Cyber Working Group has built on the work in Chapter 7 of the earlier document. This paper has been designed to be a «Consideration» guide on preparation for and reacting to a cyber-attack, for Securities Services industry participants.

The intent is to set out several things that a securities Market Participant should consider. These are not Best Practices as the breadth and depth of each individual firm needs to be weighed against what each firm needs to risk manage and the solutions proposed are only one set of proposals, which may be inappropriate for a particular firm or scenario. The Working Group believes that the bar can be lifted across the industry by firms understanding and taking these Considerations into account in their own incident management playbooks.

The research has shown that the actions of different parts of the value chain would not be substantially different during an incident. The vast majority of actions that would be taken by a Central Securities Depository (CSD), which is affected by a cyber incident, would be the same as those taken by a custodian bank serving one or many markets. The paper explains, at the various stages during an incident, what things need consideration. Where there are different actions to be taken by a particular Market Participant these are highlighted in the relevant section. One important perspective of this paper is to suggest Considerations to firms that are not directly impacted by a cyber incident but need to react to a compromised firm that they do business with as part of the custody chain.

There are several actions and preparations that firms can undertake in advance of any actual incident (operational or cyber) that will allow for a better response by both the compromised and non-compromised parties. The Working Group believes that testing the plans regularly and playing through extreme but plausible events will assist the industry in raising the bar.

Crisis management activities lend themselves to being time-boxed within an overall event, irrespective of how long an event occurs. Under that construct, the expected parts of each participant are laid in a generic timeline of «Incident Day» to «Post Mortem» for both the Compromised Party and the Non-compromised, but affected, members of the value chain.

In reading the document the key tenets are repeated: good plans, clear communication, flexibility and ownership of issues and their resolution. These are as important to the resumption of 'business as usual' as the best Information Technology solutions.

The Working Group requests that each institution reads the whole document, explores which of the Considerations are relevant for their firm and takes the preparatory steps needed so that if they, or part of the value chain that services them, are compromised, the firm has documented and has tested its response plan.

2. Cyber Landscape - The Big Picture

In its 2018 *Global Risks Report*, the World Economic Forum (WEF) ranked cyber-attacks as third in «likelihood» and sixth in «impact» of identified, globally-impactful risks (Figure 1). In the WEF 2020 survey (Figure 2), the «likelihood» ranking decreased due to the increased focus from supervisors and financial institutions. This focus has resulted in increased spending on deploying defences, awareness, and testing. However, given the interconnectedness of the global financial system, the impact of a cyber event remains high. In the 2020 Allianz Risk Barometer, the cyber threat to businesses around the globe was listed as the number one threat.

The introduction of new / emerging technology has extended financial services to excluded or underserved individuals, enhanced customer experiences, increased efficiency and lowered transaction costs as well as provided more diverse financing to businesses. While providing these benefits to the financial services sector, it has also served to increase the potential impacts that a material cyber event may cause to the stability of the financial markets.

CSDs and Custodians are charged with the safekeeping and management of the physical and electronic assets of its clients. These assets and the access to these assets are the foundation of market liquidity. Therefore, the rapid but safe recovery of business operations from a material event, cyber or otherwise, is paramount. The following examples of cyber events have highlighted the type of real impacts that a cyber event may have on the financial services sector:

a. In February 2016, the Bank of Bangladesh cyber heist led to the loss of USD 81 million
b. In June 2017, the NotPetya attack exploited unpatched Windows devices to affect banks, payment systems, power plants and other market segments across the globe
c. In September 2017, Equifax was targeted by a cyber-attack which led to the exposure of the personal records of 147 million individuals
d. In May 2018, Banco de Chile suffered a USD 10 million theft after an attacker used destructive malware as cover for fraudulent SWIFT transfers
e. In July 2019, Remixpoint, a Japanese crypto-currency exchange, halted services after it discovered the theft of USD 32 million in digital currency
f. In August 2019, Brinnance, a Malta-based crypto-currency exchange, became the victim of a ransomware attack where criminals demanded 300 bitcoins (USD 3.5 million) in exchange for its KYC database

Cyber-criminal organizations are also providing *crime-as-a-service* where threat groups can purchase and exchange malware that can be used to exploit organizations for financial gain.

In today's threat landscape, the most impactful cyber-attacks may originate from nation-state actors or other sophisticated cyber threat groups motivated by economic, political, and strategic reasons. These threat actors use Advanced Persistent Threat (APT) tactics to gain information on a target organization, develop and deliver malware designed to take advantage of that organization's systems, and conduct activities that best meet the actor's

objective. As the attack types are varied, the term «cyber-attack» could represent those activities that are a precursor to the final execution of the attack[2] including:

- scanning or other reconnaissance activity
- the injection of malware on systems
- the extraction from, deletion, or removal of data on a target system

Figure 1: Global Risk Perception WEF 2018

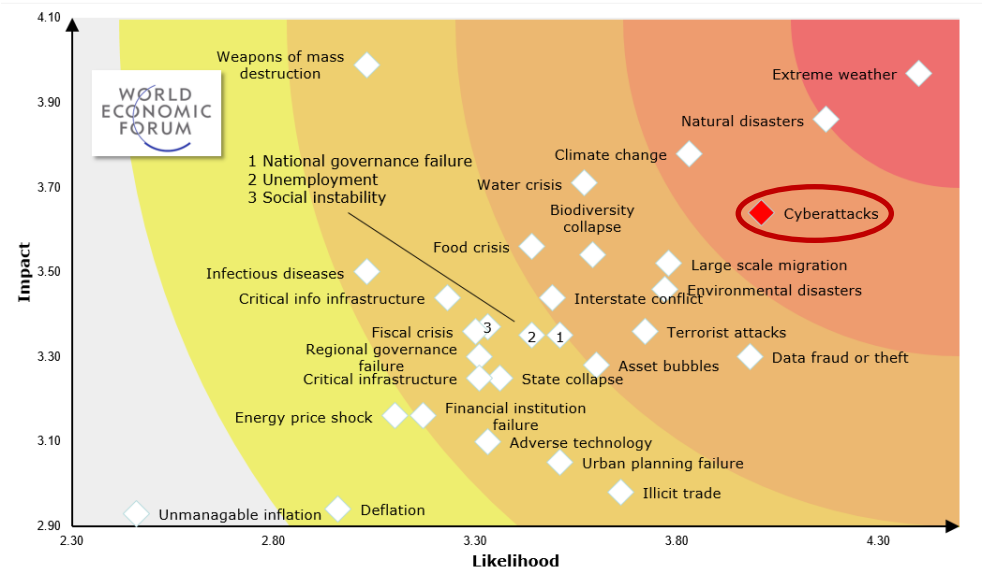
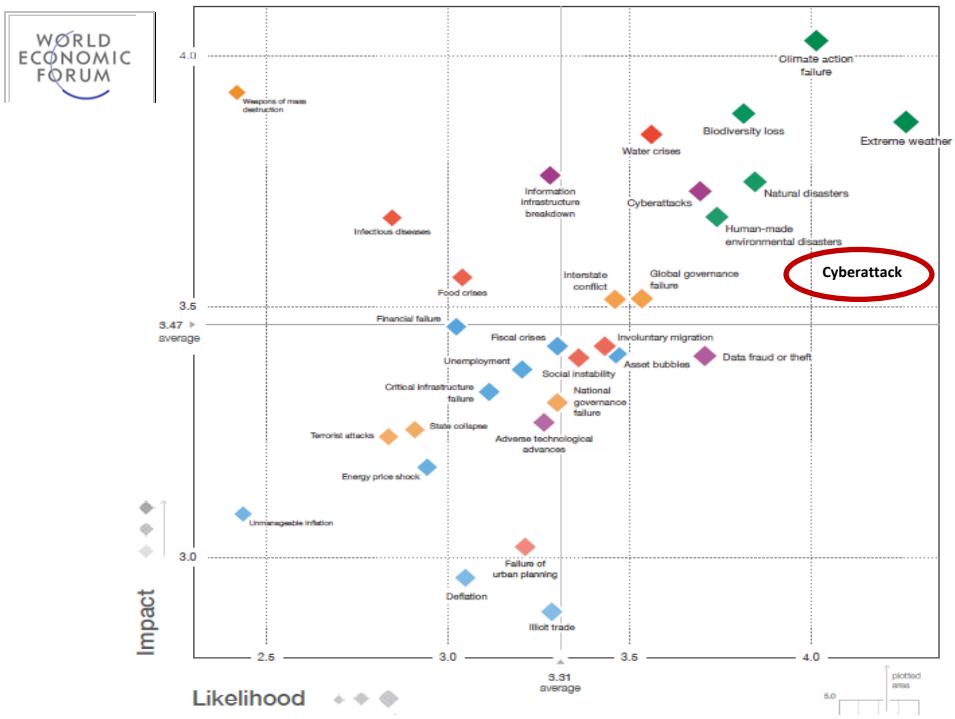


Figure 2: Global Risk Perception WEF 2020



[2] More information on the Lockheed Martin Cyber Kill Chain can be found at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

3. The Cyber Threat and the Context Pertaining to the Securities Servicing Market

Securities Service providers provide custody and enable access to many of the financial assets traded on financial markets. In this role, these organizations provide liquidity and risk management services to the entire financial services sector and, therefore, are the cornerstone of safe and orderly market functions. Given this role, these organizations implement a layered security model which consists of many cyber risk management services. Those services considered to be most impactful to securities service providers are outlined in the ISSA white paper, **Cyber Securities Risk Management in Securities Services**[3].

While many Market Participants have implemented cyber risk management programs built on industry-accepted frameworks (e.g., NIST Cybersecurity Framework, ISO 27000), the adversaries facing financial services are patient, well-funded, well-resourced and extremely coordinated. In today's landscape, it is not enough for Market Participants to mount great defence operations. They must prepare and practice «response and recovery» in the event a cyber breach materializes and plan for the potential failure or compromise of key systems.

Numerous Market Participants have developed operational playbooks that will be used in the event of a cyber-attack. It has been observed that these playbooks may focus on the firm's operations without fully addressing the requirements that it has from the supply chain. In the event that a firm's defences are compromised through a cyber incident, the effects may be much wider than the impacted firm due to the interconnectivity of the Market Participants.

The information that follows outlines risk areas that Securities Servicers should consider in their own playbooks. If they have not considered these points, the Working Group urges the firms to supplement their playbooks in order to - together as an industry - enhance the sector's preparedness for cyber-attacks. This paper also addresses the Considerations that firms that are not compromised, but are impacted, should be aware of.

It is recognized that every event is likely to be unique. Attack vectors, knowledge of what is occurring, severity, length of time until resolution and market timing are all variables in any cyber event. Therefore, whilst the proposed Considerations are the working group's views of what actions should be taken, there may be situations and circumstances which lead to a different set of behaviours. Therefore, all Market Participants should have access to the required expertise to decide the optimum response in the event of a specific incident.

It is also recognised that sharing information is key to the fast and effective prevention and detection of attacks. Similar organizations may be targeted by the same Threat Actor either in the same way or through a different campaign. The efficient sharing of indicators of compromise (IOC) and other threat intelligence is therefore extremely important to the defences of all institutions.

[3] The 2018 ISSA Cyber Securities Risk Management in Securities Services can be found at: https://www.issanet.org/e/pdf/2018-10_ISSA_Cyber_Risk_in_Securities_Services.pdf

4. Considerations for Market Participants

4.1 Introduction

These Considerations are based on a scenario where a Market Participant is impacted by an operational incident resulting in a multi-day outage. The Working Group believes that the same recommended Considerations would generally be expected irrespective of the reason for the event. The terminology of Compromised Participant has been used throughout this document to describe the party undergoing the cyber-attack.

At the start of the incident, the length of the outage will be unknown. Whilst events, such as a technology or change management failures, can result in multi-day outages, there is a higher probability that a cyber event will do so. In addition, the size or location of the Market Participant should not invalidate these Considerations as they may be implemented in all Securities Servicer firms, where the risk warrants. In an example where a large CSD has been compromised, the market impacts could propagate across the global financial services sector. The scale of market impacts may likely be different if a small local custodian in a small market is impacted. However, the Working Group has endeavoured to ensure the Considerations will be applicable in each scenario.

4.2 Expected Minimum Standards

Each Market Participant should have an up-to-date set of system and process flows available. These may be reasonably static given that the structure of the Market Participant's systems and daily processes are rarely changing. Regardless, these should be reviewed on a periodic basis (e.g. every six months) to ensure that they are still valid and current.

Key areas to consider should include:

- At a minimum, a Market Participant should have a clear process and responsibility matrix (e.g., a RACI[4] document). This should include the documented procedures of the Market Participant and, where required, be shared with the CSD's or Custodian's members / participants and regulators. It is expected that the recipients familiarize themselves with the documents and the consequences for their own firm.
- The exact nature of the matrix should reflect the realities of the Market Participant's processes and technology. For example, Fixed Income (FI) may use a different processing system than Equities. However, both may use the same client and instrument databases. Depending on the nature of the incident on the compromised CSD's or Custodian's business area, there could be different paths for actions to be taken (e.g., FI settles as normal but Equity settlement is affected; no products are able to settle).
- Before an incident, system and process flows can be used as the basis to create «Business Impact Assessments». The Business Impact Assessment can be used to determine the operational impact an outage may have to the firm and the financial services sector. For example, this may show whether an incident may cause a settlement delay which could affect FX, funding, or cash balances.
- As part of their playbooks, Market Participants should consider the impacts of an outage of their critical third party providers to their firm's operations. This provides reasonable assurance that responses are tested prior to a potential event.

[4] RACI is defined as (R)esponsible, (A)ccountable, (C)onsulted, (I)nformed.

- Plans should be regularly tested based on different market variables including: an institution's size, products traded, access to trading venues, and systemic importance. Significant changes in the threat landscape may also increase frequency of this testing. Testing should, at a minimum, be conducted annually and cover the Market Participants' internal and external communications and various incident scenarios. Well tested plans will also decrease the operational friction of those activities that would otherwise occur at the time of an event. The after actions (i.e., wash-ups) from these exercises should be used to refine the communications and playbooks for the next exercise.
- All Market Participants should conduct «table top» exercises involving senior leadership, at a minimum, annually. When possible, financial institutions should consider participating in external and sector exercises (e.g., those coordinated by industry associations such as SIFMA, GFMA).
- All Market Participants should look to increase the complexity of their table top exercises to further approximate what is an «extreme but plausible» event to occur during a real incident. This may include losing communication channels that are normally used to inform internal and external parties.
- Firms may also consider how timing[5] may impact their response to a cyber event

A template for a table top exercise for the failure of a critical operating counterpart can be found in Appendix 1.

In the normal course of business, a CSD should consider and agree with their participants that the participants will hold electronic copies of any transactions that they have sent until settlement finality has occurred and has been acknowledged. This would facilitate transaction replay if the CSD systems have an information corruption event.

If a large or regional CSD cannot perform settlement for an extended period (e.g., > 1 day), there may be far reaching market implications. For example, an outage that is longer than one day may have significant daily funding impact in the Commercial Paper market. Given that rules and law differ by country, it is recommended that CSDs examine their rulebooks to identify their options for this outage type (e.g., invoking a non-settlement day).

A scenario in which there is a difference in the market implications of an incident is when an incident continues beyond a settlement cycle where there is a higher risk of contagion to other markets. For example in the European markets the CSDs are impacted by cross border settlement, T2S (both for funding and settlement) and the bridge between the ICSDs. This interaction may cause an issue in one market to affect the funding and collateral availability in other settlement venues.

It should be noted that CSDs within the Target2Securities (T2S) system (and T2S itself) can only roll back to the end of the previous day. This means that any possible effects of an incident which occurred on T-1 and identified on T can, in most cases, only be managed through a claims process rather than rolling the system back. Depending on the incident and on its effects, where the T2S CSDs or T2S fail over multiple days, trades which are in the systems and are considered to be valid (meaning that there is no data breach, no loss of data and trades were not tampered with or altered) will be settled with settlement and value date equal to the current business date instead of the originally intended settlement date. If trades have been affected by the incident, T2S and / or the T2S CSDs may be required to ask their clients to re-instruct the trades.

[5] Time of day, day of week, week of month, month of year may significantly change the response of a Market Participant to a cyber event.

4.3 Considerations for a Compromised Participant

This section lays out the Considerations that the working group identified along the timeline of the «Incident Day» until «Post Mortem» for a Compromised Participant. Where the practices differ due to differing market functions of a Market Participant, this is highlighted. In addition, the actions are grouped under logical headings such as «Communication» and «Process Flows and Business Impact» for ease of reading. The order of these headings does not reflect any implied priority but are to provide coherence to the paper.

4.3.1 Incident Day

Communication

The intent (i.e., accidental, malicious) and cause (e.g., cyber, operational change) of an outage may not be known at the start of an incident. In most instances, a cyber incident will not initially be assumed unless clear evidence suggests otherwise (e.g., ransomware). Therefore, the initial indication of a material operational event is when either the organization or its clients experience irregularities in normal operations. At this point, the Compromised Participant will engage in troubleshooting activities to identify the cause of the incident, confirm what activities are required to fix it and when those activities may occur.

Where it is identified that the event is a result of a cyber-attack, the timing and content of any communication may be dictated by local law or regulation. Therefore, each Market Participant should be aware of the reporting requirements within their jurisdiction. Notifications should be issued as soon as practicable following the point at which the Compromised Participant has determined the incident to be material, having considered those factors that may be affected by the outage (e.g. market deadlines for securities and cash/currency) in that materiality assessment. Additionally, by this point, the Executive and internally required Board Committees should be notified and where necessary involved.

In the event of a cyber-attack, the Compromised Participant should conduct all incident reporting as required by rule or law. As an effective practice and to support the resilience of the Securities Services sector, the Compromised Participant, where appropriate, should contact:

- The Compromised Participant's own participants / members / clients: The communication should include the potential level of impact so that these entities can perform their own impact assessment. The Compromised Participant may have a contractual obligation to inform clients within a specific time frame. This should be adhered to but should not favour one client over another
- Relevant trade associations and industry bodies (e.g., AGC, AFME, ASIFMA and SIFMA) so that they can initiate the appropriate Incident Management Groups
- The national and regional cyber incident sharing bodies (e.g., ENISA or FS-ISAC) who will communicate quickly to inform non-compromised firms.
- Supervisors and Regulators as required by rule or law
- Central Banks[6] (where applicable)
- The Compromised Participant's marketplaces and impacted FMIs (e.g., exchanges, CCPs) where applicable. The Custodian may need to inform an exchange in specific situations (e.g., the Custodian has suffered a catastrophic

[6] It is recognized that Custodians would rarely need to inform the Central Bank unless the Central Bank is part of the local supervisory regime

failure). The local Central Counterparty or Clearing House (CCP) should be informed if the associated CSD is impacted. This equally applies if the Compromised Participant is a large Custodian where there is the potential that the whole market or a significant market segment could be impacted

- If the Compromised Participant is a Custodian then the Custodian should inform the affected CSD(s) who will inform their members.

  For example: The Compromised Participant is a regional Custodian who is a settlement member in 5 markets, and for three of those markets the market interface they use to settle was impacted by the incident:

  1. In this case the Custodian would inform the three impacted CSDs who would inform their members
  2. The Custodian would inform its clients who were active in the three impacted markets
  3. The Custodian may choose not to inform their other clients who only use services in the two unaffected markets.
- Other organizations outside of local financial regulators may need to be informed
- If the Compromised Participant is a CSD, it should inform any Issuers and their Registrars in the event they have any pending Corporate Actions or Elections
- If the incident involves loss of Personal Identifiable Information then informing the «Privacy» Regulators rather than the banking regulators and supervisors needs to be considered

The timing and content of the communication may be dictated by local law or regulation. Therefore each Compromised Participant should be aware of the reporting requirements within their jurisdiction. Examples of these requirements can be found in Appendix 3. Communication should be issued as soon as practicable following the point at which the Compromised Participant has determined the incident to be material, having considered those factors that may be affected by the outage (e.g., market deadlines for securities and cash / currency) in that materiality assessment.

Due to the fluidity of available information during the cause of an incident, it is recommended that the Compromised Participant consider a communications plan which includes:

- The group of business leads responsible for firm messaging (e.g., business operations, general counsel, communications, public relations, information technology and human resources)
- The information that is confirmed regarding the incident
- The development of internal and external communications regarding the event
- The communication vehicles to be used for messaging

Communication from the Compromised Participant should include (to the extent known at the time of announcement):

a. Validated and verified information approved by the Compromised Participant's governing body, and what actions have been taken to date
b. When the next communication will be provided (which would minimally include communication ahead of funding deadlines, at close of business and before start of business the following day)
c. The extent to which the notification can be passed through to the Compromised Participant's clients and interested parties without modification. All participants should be aware that any information shared should be considered as public information unless explicitly stated

d. The communication should provide pertinent information from the business impact assessment as soon as possible
e. If available, any technical information to enable other participants to protect themselves
f. Information about any impact on in flight transactions
g. Details of any requests of Market Participants (e.g., provision of instructions already sent to assist CSD's reconciliation)

Where the Compromised Participant is a CSD, the following additional information should be provided:

a. Information to the Market Participants related to any extensions being considered
b. Whether the CSD anticipates closing and the notice it will provide before re-opening
c. Information on the approach that will be taken to facilitate pending Corporate Actions
d. Whether the Custodian should interact directly with the Issuer / Registrar or use the CSD as an intermediary for pending elections

Where the Compromised Participant is a Custodian, the following additional information should be provided:

a. Whether the cyber incident could spread or is impacting clients (for example, if there were segregated accounts held at the CSD operated under an «Account Operator» model). The Working Group believes that non-compromised firms would act as though the incident could spread regardless of the Custodian communication to the contrary. It is therefore recommended that Non-compromised Firms should make their own impact assessment using the Compromised Firm's communication/ assessment
b. Whether the Compromised Participant has asked for any extensions at any impacted CSD(s) and whether they have been accepted
c. Where known, information on which trades are impacted by the event. This may include the percentage of trades that have been sent to the CSD and those held back

Process and Business Impact Assessment

Every Market Participant should have an up-to-date set of System and Process flows available. These, in conjunction with the critical timeframes and deadlines for each business's normal day, should be used as the basis to create «Business Impact Assessments» (BIA). These can then be used as the baseline for determining potential scenarios that can affect business operations and understand the business impacts they could cause if realized. This should show what settlement delays could occur if an incident affects FX, funding, and cash balances. These outcomes should be known and the Market Participant should provide an explanation of the consequences of each. The possible scenarios that are developed through the Business Impact Assessments can be used in tabletop exercises and therefore decrease the operational friction that could occur during an incident. This will increase the likelihood of a rapid but safe recovery of the Securities Services sector.

All Market Participants need to make a risk based business decision whether to «disconnect» from the Compromised Participant. Given the number of potential different scenarios and Market Participants the Working Group makes no recommendation on the path to follow, but rather that it is an important Consideration to have planned for.

For Market Participants who are CSDs, the following are the key points to consider in the Process and Business Impact Assessments:

- The most important information for a Market Participant from the BIA concerns the settlement status. Once understood, the CSD should make information available about those submitted trades that will settle
- The Compromised Participant should have the ability to produce MIS to show what the situation is, or was, at the last known correct / restore point if that is possible. This MIS should show the current status of trades in the settlement cycle. This information could be provided during a cyber event to all participants and their clients (via the Custodians)
- The CSD should decide and communicate whether a Non-Compromised Participant should continue to send transactions, or hold them. This is as the CSD is controlling and communicating the incident. This decision should be made with a clear view of the BIA.
- During an incident, the Compromised Participant should state what their prioritization rules are for settlement instructions. There are a variety of methodologies for this, for example:
    1. A CSD will attempt to process all existing instructions first where settlement date has been reached, then take new instructions in settlement date order
    2. Alternatively a CSD may prioritize the processing of systemically important high value transactions
- The Compromised Participant should look to produce reconciliation files for the Market Participants as soon as possible
- It is the Working Group's recommendation that the prioritization should generally be by settlement date, and then by highest value transactions within that settlement date as a proxy for market stability. Depending on the circumstances, a Compromised Participant may use algorithms or business decisions to prioritize in a different manner to optimize the whole market outcome

While the Working Group did consider the possibility of the CSD contacting Market Participants to determine a processing methodology, it was considered impractical for the CSD to accommodate all requests and, therefore, discarded as a viable option.

Custodians should also be accountable for maintaining their own BIA and have the ability to use their own systems to indicate the time of an outage, or impacted trades based on their internal systems records (e.g., the last update received from CSD). It is not expected that a Custodian's clients can do the same if there is a problem at their Custodian.

For a Custodian, the following key points about Process and Business Impact Assessments should be considered:

- The Compromised Participant should try to settle the maximum value of settlements within the day to minimize the impact on their clients and the financial markets
- In the event the CSD allows partial settlement, the Compromised Participant should utilize it
- A number of Custodians offer «Hold and Release» functionality on omnibus accounts and often only release delivery instructions to the CSD following disposition checks in those accounts. This is not the case for segregated accounts at the CSD. Custodians may also «hold» receipt instructions to allow for credit checks to confirm the client has a sufficient credit line to accommodate the stock receipt (as cash will need to leave the account for settlement). A Custodian should

confer and review with clients all transactions on hold to see if they should be released. Where it was a «client hold», release must be agreed with the client

- The key requirement from Market Participants is the ability to reconcile transactions to a point of time. This may be easier for batch driven systems where the transactions are either processed in the batch or not processed (unless the event occurred mid–batch), but for real time systems it could be harder to establish the time of failure and the instructions that were not completed.
- With respect to reconciliation files, it is anticipated that the normal statement cycle (e.g., MT950 for cash, MT535 for stock, MT537 for open transaction reporting) and intraday settlement updates (MT548) will continue where possible.
- The Compromised Participant should inform their clients of impacted transactions once that is known

Where the Compromised Participant is a Custodian, the clients should continue to send instructions to the Custodian as long as the incident has not affected the integrity of the Custodian's inbound communication channels. The Custodian should have the capability and capacity to hold these messages until it is able to start processing them.

Staffing Considerations

The Compromised Participant should look at the following staffing Considerations:

- Assess staff resourcing requirements considering the potential for increased reconciliation differences, re-instructing and enhanced monitoring including of duplicates
- Ensure that client service teams are available to provide support for the likely increase in client queries
- For client communications, a FAQ template will assist the quick generation of client ready communications (Appendix 4).

Technology Considerations

The following technology practices should be considered:

- In advance of an event, Market Participants should assess their technology capacity and capabilities should volumes require rapid throughput
- If a trade can settle on settlement date, all efforts should be made to meet this date
- Technology capacity should have the ability to process the majority of transactions by the end of day. This is dependent on the market cut-offs, including the ability to request an extension within a market

4.3.2 Incident Period

Communication

It is anticipated that during the incident period the Compromised and Non-Compromised Participants would continue to inform the same list of recipients as outlined in the section «Incident Day, Communication» above.

These updates should be ongoing and must, at a minimum, be ahead of funding deadlines, at the close of business and before the start of business. A communication should precede any new significant information (e.g., if the settlement cycle is going to restart or instructions sent).

In addition to updating the information from the Incident Day, the Compromised CSD or Custodian should consider, if not already covered in the Business Impact Assessments:

- An approach to market discipline / penalties and the suspension of these practices
- Confirmed details of any corrupted transactions
- The approach and strategy for replaying transactions from a specific time
- The articulation of a resumption strategy considering appropriate timings relative to market deadlines, cash management and Treasury team input

4.3.3 Resumption Day & Clean up period

Communication

It is anticipated that during the incident period the Compromised Participant and Non-compromised Market Participants will continue to inform the same list of recipients as outlined in section «Incident Day, Communication» above. It is recommended that active communication continues until all trades are settled and Business as usual is achieved.

Before resumption the Compromised Participant should include:

- Re-start timing, including an assessment of starting during the day versus a new day. This should be determined on the basis of the market cut-offs. If the start time is intraday and then availability of liquidity to the participants either through the normal channels or the CSD's credit policies, needs consideration
- Confirmation of the enhanced monitoring procedures including connection validations and reconciliation processes
- Extra support available for the Market Participants / clients (e.g., participant and client queries)
- Timing of any re-introduction of market discipline measures
- Target date for the formal lessons learnt document to be published

Processes and Business Impact Assessments

Where the Compromised Participant is a Custodian, they should ask the CSD for an extension if this allows them to settle a significant value of transactions. The regulator(s) should be notified where appropriate.

CSDs should attempt to accommodate requests for an extension if it is within their capability to continue to run their daily business. It is recognized that there are a number of factors and constraints (such as T2S funding deadlines in Europe) that may affect the ability to extend and that the decision rests with the CSD.

4.3.4 Post Mortem

The Compromised CSD or Custodian should share the lessons learnt with the community and update the Business Impact Assessment based on its experiences.

4.4 Considerations for a Non-Compromised Participant

The Market Participants who have not experienced the cyber event directly may still be impacted by the event if they interact with the Compromised Participant. This section highlights those areas which the Working Group believes are of importance, but also recommends that the Market Participants are aware of the previous sections, especially the prior section discussing the Compromised Participant settlement priority options.

4.4.1 Incident Day

Communication

After the incident is communicated to the Compromised Participant's own clients / participants / members, those parties should make their own internal assessment. Depending on the impact to their own clients and business, and their own communication policies, they should then communicate to:

1. Their clients about the impacted services
2. Their regulators depending on impact and severity of the Compromised Participant's incident and the services provided to the Non-compromised Party
3. Their Executive and Board Committees

If the Compromised Participant is a CSD and it has issued a notice for onward delivery to its end clients, this should be used as the basis for communication to the participants' / members' clients. As noted, any communication issued should be considered public unless explicitly stated.

If the Compromised Participant is a Custodian then the message flow would be:

1. Custodian to CSD
2. The CSD has accountability to communicate its participants / members which in some cases may be above the Custodian in the securities servicing chain
3. Custodian to the Custodian's Clients and
4. From those clients to the clients of those clients.

The communication should include key actions and decisions on whether client instructions:

1. Will continue to be sent to the Compromised Participant or held, or
2. Should continue to be sent to the custodian.

These are useful to forecast funding requirements.

Process and Business Impact Assessments

It is recommended that in respect to client settlement instructions that these should continue to be sent to the Custodians. When reopened, the CSD should decide and communicate if firms should throttle the sending of instructions.

Custodians should have the ability to send (or resend) instructions by settlement date. This would be useful to avoid capacity constraints. CSDs should have the capacity to consume a day's worth of trades before it closes. The other alternative is for the CSD to provide an extended cut-off to ensure all transactions for that business date can be given the ability to settle, taking into account funding and liquidity constraints.

Cash Management, Funding and Liquidity Considerations where a CSD is the Compromised Participant

Market Participants should run cash projections, considering settlements and unprocessed transactions, and these should be run against the CSD, as well as the participant's clients to ensure that credit decisions can be made. There may be the requirement to post collateral or cash to offset the impacts. Custodians would have to estimate the exposure to the compromised CSD if there is no visibility and the CSD cannot tell them which transactions have settled. This estimate can be made by, for instance, utilising pending transaction reports for trade settlement and income events for the appropriate settlement date. If the CSD can inform the participants of the cash projections it should do so.

The presumption is that all good trades should settle. The Custodian should aim to find liquidity and funding to allow settlement. In extremis, if this cannot happen an agreement must be made between the two parties to the trade and the CSD before cancelling any trade.

Some Custodians provide their clients with automated «Cash Sweeps» where client balances are swept (automatically) to a money market fund or other short term investment vehicle. In cases where these sweeps are executed based on future matched settlements, then the Custodian should look to review their sweep process in the light of a CSD having an incident.

The Custodians should have reporting in place to identify and inform clients that need to fund their positions due to offsetting settlements not completing as anticipated.

If the market's CSD had an incident and a subsequent liquidity impact the Custodian would likely absorb that cost of the intraday liquidity. The cost of intraday liquidity in this situation is not obvious and only a few Central Banks (e.g., US Federal Reserve and others) charge an intraday cost for liquidity usage. The Working Group believes that a CSD having an incident would be unlikely to make their clients whole for liquidity costs.

The other element to consider is where the liquidity is residing for cash projections and funding calculations. For example, a FX position may have not moved from the firm's cash nostro to the CSD accounts and may need to be reinstructed or it has moved to the CSD accounts but cannot be used for funding purposes (e.g., frozen at the compromised CSD). Custodians should ensure that they fund their positions taking this information into account.

Credit Risks Considerations where a CSD is the Compromised Participant

The Custodian will need to look at the emerging credit conditions of their clients. These may be worsened by the situation if a client has a particular concentration in an affected market. In addition, consideration should be given to the possibility that:

1. A Custodian may have executed an FX transaction to allow the funding of settlement in a different market creating an FX position which should be part of any credit calculation made by the Custodian
2. The creation of an FX position in itself may not be an issue but as the market value moves over time the FX position may create an exposure if the settlement does not occur over an extended period

If there is an incident with a CSD that impacts clients' available credit, the Working Group determined that the Custodian could extend credit lines for intraday credit needs provided that they have the information to do so. This would be added to the daily credit lines and determined on a client-by-client basis. If the credit exposure moved from intraday to overnight, there would be more impact and the Custodians should further assess and talk with individual clients.

Additionally, the Credit Control Process may need to be reviewed especially if the client had a relatively adverse rating. In some cases, the Custodian's credit processes are set up to allow the offsetting of credit across countries / settlement locations (e.g., RVP in one country is allowed on the basis that a DVP will cover the credit exposure in another country and currency). If the affected CSD is down and the cash is not released, an exposure created by the RVP is not offset. As a consideration, the Custodian should review their Credit Assumption models once they are informed of the issue. It is difficult for the working group to suggest a best practice for managing this exposure as it will depend on risk appetite and specifics of the situation.

The participants should assess the potential impact on FX operating models and standing instructions and consider disabling «auto-FX». The implications of disabling auto-FX are complex. In all instances the recommendation is for the Custodian to agree with their end client the approach for individual FX transactions.

If the FX is not cancelled then the client of the Market Participant will have an FX position with an unknown offsetting securities settlement date, they potentially have limited ability to manage that FX risk, and no asset. However, there are different implications of taking this approach depending on whether the client is buying or selling the security in a different currency and the effect on settlement. It was also noted that FX movements can cause significant losses if done on different days or if the FX trade is cancelled only to be re-instated when the affected CSD reopens.

Consideration should also be given to the impacts on credit of continued trading in the market if the exchange is functioning and the exposures that this creates or mitigates.

Corporate Action Considerations where a CSD is the Compromised Participant

As referenced in earlier sections, Corporate Actions have a similar requirement to in-flight settlement instructions and the expectation is that the CSD would provide information on its approach in its initial market communication. The Custodians should respond to this plan to ensure clients are not disadvantaged, including issuing Notices of Liability to other Market Participants if required. If the Compromised Party is a CSD then Income and Corporate Action cash proceeds may be delayed throughout the chain.

In respect to Corporate Action notifications, CSDs are not the only source of this information and it is expected that even if a CSD is compromised that other sources will be used to inform the Custodian's clients of notifications.

When it comes to elections, it should be known whether the Custodian should interact directly with the Issuer / Registrar or use the CSD as an intermediary. If it is not clear, then the Custodian should clarify how it can mitigate the risk that the end client does not miss an election. The Custodian and CSD should have open lines of communication for Corporate Actions and Voting, but the onus rests with the CSD to ensure that their communications cover an approach for upcoming Corporate Actions, and that communication occurred with the issuer(s).

With regards to Voting, it is the Working Group's view that the Custodian should intend to have the capability to process the instructions manually if required to protect the clients' interests. In some cases where a large number of votes are to be tabulated, this may not be possible and can only be executed on a best efforts basis.

Contractual versus Actual Settlement and Income Postings – Continue or Reverse – Considerations where a CSD is the Compromised Participant

The contractual versus actual settlement recommendation is aligned to the afore-mentioned FX consideration. There is no recommendation beyond making sure that the approach of a Custodian is covered in its planning process. This topic covers several

different factors which are as unique as a firm's business. They include but are not limited to:

i. The liquidity impacts
ii. The potential timeline of the incident
iii. Credit Risk Management's input,
iv. The contractual obligations and commercial considerations of suspending contractual settlement
v. Impacts to the movement of the prudential ratio and the regulatory reporting requirements
vi. And when to talk to the clients

Staffing Considerations

The Non-compromised Parties should assess staff resourcing requirements considering the potential for: increased reconciliation differences, re-instructing and enhanced monitoring including the processing of duplicates.

It may be necessary to reassign staff to support client service teams due to the likely increase in client queries. To help support client teams, the working group recommends that a FAQ template be created in advance using the content of this paper as a baseline. A pro forma version is included in Appendix 4.

Technology considerations

In advance of an event, Market Participants should assess their technology capacity and capabilities should volumes require rapid throughput. The recommended practice is if a trade can settle on settlement date then every reasonable attempt should be made to meet this date.

Technology capacity should have the ability to process the majority of transactions by the end of day. This is dependent on the market cut-off, including the ability to request an extension within a market.

4.4.2 Incident Period

Communication

It is anticipated that during the incident period the Compromised and Non-Compromised Participants would continue to inform the same list of recipients as in section «Incident Day, Communication» above.

These updates should be ongoing and, at a minimum, be ahead of funding deadlines, at the close of business and before the start of business or when significant new information is known (e.g., if the settlement cycle is going to restart, or instructions sent).

In addition to updating the information from the Incident Day, the Compromised Participant should consider communicating:

1. The approach to market discipline / penalties and the suspension of these practices
2. Communicating information regarding any corrupted transactions
3. The approach and strategy for replaying transactions from a specific time and
4. The articulation of a resumption strategy considering appropriate timings relative to market deadlines, cash management and Treasury team input

4.4.3 Resumption Day and Clean up Period

Communication

It is anticipated that during the incident period the Compromised and Non-Compromised Participants would continue to inform the same list of recipients as identified in the section «Incident Day, Communication» above .

In addition to the Compromised Participant communication, the Non-Compromised Participants should confirm that they have recovered in line with the Compromised Participant's plan, inform their clients of any changes and the timing of those changes with respect to auto-FX and contractual settlement.

Active communication is recommended until all trades are settled and Business as usual is achieved.

4.4.4 Post Mortem

The Non-Compromised Participants should adapt their play books from the experience, share the lessons learnt with the community and update their Business Impact Assessments.

Appendix 1 –A Template for a Table top Exercise for the Failure of a Critical Operating Counterpart

Phase	Assess	Considerations
Governance	Response to Disruption Event will vary based on the severity of the outage and based the RACI established in the section 4.2 Expected Minimum Standards	Crisis Event Level 1 – Critical Crisis Event Level 2 - High Impact Crisis Event Level 3 -Medium Impact Crisis Event Level 4 -Low Impact Crisis Event Level 5 - No Impact
Initial Response	Identify if your business is impacted	1. Isolate application and inform primary contacts as per the RACI 2. Identify Impacted Users 3. Understand the threat
Impact Assessment	Identify the impact to your business after the impacted applications and users have been isolated and understand the situation	1. Which business critical process is or will be impacted? 2. What is the systemic AUC and transactional impact? 3. Will client SLA's be breached? 4. Who are the critical stakeholders?
Containment	Containment Options are specific measures or actions which can be taken in response to a cyber threat, in order to «contain» that threat and protect network and assets.	1. Forced Password Reset 2. Block /Quarantine Inbound Emails and Attachments 3. Disconnect select B2B Connections 4. Segment Impacted system from Network 5. User Workstations rendered unavailable 6. Disable inbound and outbound file transfers 7. Disable critical applications 8. Prohibit staff access to the internet
Communication Planning	Once the critical internal and external stakeholders have been identified, work with Public Affairs and Legal to agree the messaging. The Working Group recommends the «Considerations for a Compromised Participant, Incident Day, and Communications» as a guide.	1. Who should you communicate with? 2. By when must you communicate with them? 3. What method of communication should be used? 4. Who should communicate with them? 5. Work with Public Affairs and legal to draft message 6. Business approval required 7. Employees should not respond to media enquiries without advice from Public Affairs
Recovery Planning / Review	Before determining if organisation can return to «Business as Usual» status, recovery review needs to take place	1. Has the threat been contained? 2. Has the threat reason been eradicated from the network? 3. Are critical business systems still affected? 4. Assessment of impacted systems 5. Continuity of Business plan should be referenced for critical applications or processes 6. Establish and communicate re-establishment of «Business as Usual» timelines

Phase	Assess	Considerations
Post Incident Review	To assist the organization and record the knowledge gained from the process of the cyber event and to share and use the knowledge derived from experience.	1. Identify recommendations and lessons learned from the event 2. Categorize event – Personal Identifiable Information / Info Sec / Data Breach, Insider Threat, Destructive Malware, 3rd Party Compromise 3. Document and share findings 4. Analyse the findings 5. Update the relevant artefacts or processes 6. Store in the relevant cyber security repository

Appendix 2 – Glossary of Terms

Term	Definition
Advanced Persistent Threat	A set of structured continuous and sophisticated attacks that are used to compromise a targeted entity
Anomaly-based monitoring	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations
Authenticated Vulnerability Scanning	A scan that uses system credentials to discover vulnerabilities that may exist on an Information System
Authentication, Multi-factor	Authentication using two or more of the following factors: ▪ knowledge factor, «something an individual knows» ▪ possession factor, «something an individual has» ▪ biometric factor, «something an individual is or is able to do»
Authentication, Single-factor	Authentication using only one of the following factors: ▪ knowledge factor, «something an individual knows» ▪ possession factor, «something an individual has ▪ biometric factor, «something an individual is or is able to do»
Authentication, Strong	Authentication using one of the following factors more than once before allowing access to the Information System: ▪ knowledge factor, «something an individual knows» ▪ possession factor, «something an individual has» ▪ biometric factor, «something an individual is or is able to do»
Compromised Participant	An actor within the Securities Settlement chain, used in this survey to generally mean an (I)CSD or Custodian who is undergoing a cyber event
Cyber Event	An observable cyber occurrence in an Information System
Cyber Incident	A cyber event that jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits
Cyber Threat Hunting	The process of proactively and iteratively searching the computing environment to detect and isolate threats that have evaded existing security controls
Distributed Denial of Service	A type of cyber-attack where multiple compromised systems are used to make an Information System unavailable to its intended users
Indicators of Compromise	A piece of forensic data, such as data found in system log entries or files, that identifies potentially malicious activity on a system or network
Information System	A set of applications, services, information technology assets or other information handling components
Key Performance Indicator	A measurement that gauges how well a service is performing against its goals
Key Risk Indicator	A measurement that is used to determine the level of risk to which an organisation is exposed

Term	Definition
Market Participant	Any organisation operating within the Securities Servicing arena such as (I) CSD, global, regional or local Custodian.
Penetration Testing	The process of conducting real-world attacks against an Information System to identify security weaknesses before they are discovered and exploited by others
Phishing	A digital form of social engineering that uses authentic-looking - but bogus - e-mails to request information from users or direct them to fake websites that request information
Ransomware	A type of malicious software that prevents or limits users from accessing their system either by locking their system screen or files until a ransom is paid
Spear phishing	A digital form of social engineering that uses an authentic-looking - but bogus - e-mail to request information from a distinctive set of users (e.g. corporate executives) in an attempt to have them provide sensitive information
Tactics, Techniques and Procedures (TTP)	The three levels of behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour and procedures are an even lower-level, highly detailed description
Threat Actor	An individual, group, or organisation believed to be operating with malicious intent
Threat Intelligence	The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions and activities that offer courses of action to enhance decision making
Three Lines of Defence	A management risk control framework which consists of three levels used to provide oversight of an organisation's risks
Unauthenticated Vulnerability Scanning	A scan that attempts to discover vulnerabilities on an Information System through limited system access
Watering Hole Attack	A security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit

Appendix 3 – Examples of Regulators' Requirements

Switzerland
https://www.finma.ch/en/documentation/finma-guidance/ (search for FINMA Guidance 05/2020 Duty to report cyber-attacks pursuant to Article 29 para. 2 FINMASA)

USA
https://www.finra.org/rules-guidance/key-topics/cybersecurity#overview
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Europe (ECB)
Serious Information Security Incidents
For all Severity 1 and Critical Information Security incidents ECB incident report form has to be sent within 2 hours via PGP encrypted email to cybercrimeincidents@ecb.europa.eu.

UK
https://www.fca.org.uk/firms/cyber-resilience

Italy OES (Operator of Essential Services) the Implementing Decree 65/2018 of the NIS directive
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/Dlgs-65_2018-NIS.pdf
mandates the communication of security incidents to the national CSIRT at https://csirt.gov.it/segnalazione (link to access via Browser)

Germany
German Federal Office of Information Security (BSI) – Serious Information Security Incident on German Critical Infrastructure
Incidents with significant disruptive effect on the availability, integrity, authenticity and confidentiality of the critical infrastructure and all Severity 1 Security Incidents have to be reported with undue delay to the Federal Office of Information Security (BSI) in Germany based on the German IT Security Act. The agreed incident report has to be submitted via the BSI portal https://mip.bsi.bund.de/incidents

Japan
https://www.fsa.go.jp/en/principles/index.html#03

Hong Kong
https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi/

Singapore
MAS template for incident reporting and overall MAS guidelines
https://www.mas.gov.sg/regulation/forms-and-templates/incident-reporting-template
https://www.mas.gov.sg/regulation/cyber-security
(both links to access via Browser)

Singapore banks association guidelines on cyber simulation exercises:
https://abs.org.sg/docs/library/media-release_abs-issues-guidelines-for-cyber-security-exercises_14nov18.pdf
https://abs.org.sg/industry-guidelines/cyber-security

Appendix 4 – Examples of Frequently Asked Questions to be Considered

Frequently Asked Questions:

In the case where there is a Custodian system outage, clients will request contingency method of supporting their instructions.

When outage occurs close to cut-off, clients will ask if there are any claims as a result of late settlement due to outage. How will these be dealt with?

Client will request Custodian to outline the root cause of the outage.

In some markets Custodian is required to submit substantial shareholding reporting on behalf of client, client will be penalised by regulator in the event of failure to report or delay in reporting. Clients want to know if Custodian will bear the penalty amount if the failure or delay is cause by Custodian's system outage.

Failure or delay in releasing dividend or coupon interest to client due to system outage causing insufficient funding in client's account for trade settlement. How will Custodian compensate client?

Have you (the compromised institution) followed the SWIFT CSP?

Has there been an audit of the cyber framework in your firm recently?

Have you got a templated disclosure of your system security plan and actions?

Appendix 5 - Working Group Members

Salutation	First Name	Last Name	Contact's Legal Entity Name
Mr.	Andrew	Gray	DTCC
Ms.	Jennifer	Cryan	Citigroup
Mr.	Thomas	Koch	SIX
Mr.	Andrew	Smith	The Bank of New York Mellon
Mr.	Michael	Bem	UBS
Mr.	Jyi-chen	Chueh	Standard Chartered Bank
Mr.	Dale	Connock	Strate (Pty) Ltd
Mr.	Daniel	Coray	SIX Group
Mr.	Roberto	Degni	Monte Titoli
Mr.	Peter	Demarré	Euroclear SA/NV
Mr.	Terry	Ferrão	Citibank
Mr.	Göran	Fors	SEB Group
Mr.	Jason	Harrell	DTCC
Mr.	William M.	Hodash	DTCC
Mr.	Bhavesh	Jani	Citibank
Ms.	Emma	Johnson	Deutsche Bank AG
Mr.	Brett	Lancaster	SWIFT
Mr.	Dario	Mariotto	Unicredit
Ms.	Irene	Mermigidis	Clearstream Banking / REGIST-TR
Mr.	Colin	Parry	ISSA
Mr.	Marius-Bogdan	Pindaru	Unicredit
Mr.	Manoj	Sarangi	NSDL India
Mr.	Hariprasad	Subramani	Standard Chartered Bank
Ms.	Susan	Vismor	BNY Mellon
Mr.	Nejib	Zaouali	Clearstream