Cyber Security Risk Management in Securities Services

October 2018

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. The World Economic Forum's 2018 Global Risks report considers cyber attack risk as the third most likely and sixth most impactful of all global risks.

This document sets out the cyber attack threats to firms active within securities servicing and the risk mitigation techniques they should take to manage those threats that may lead to a material impact to the securities servicer firm or to the financial markets.

Target Audience
This document is targeted at Senior Management, Information Security Professionals and Risk Managers working within the securities services industry, particularly those working within Central Securities Depositories, Global and Sub Custodians and Securities infrastructure and utility firms.

Acknowledgements
The report 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 supplied valuable market information. The names of participating firms and the individual contributors are listed in Appendix 3. The ISSA Executive Board wishes to thank all supporters for their contributions as well as their firms having enabled their participation.

Cross Reference to ISSA's Custody Risks Report
The ISSA report entitled '*Inherent Risks within the Custody Chain'*, for short 'Custody Risks Report', was issued in February 2017 and represented a holistic review of all key categories of risk, how they impact and are mitigated within the securities services value chain.

The report included a chapter which captured Information Security Risks and provided a high level description of the causes, exposures and countermeasures with this risk type.

This report elaborates on the specific cyber risk referenced in the Custody Risks Report and describes the threat landscape, actors, threat evolution, susceptibility factors and risk mitigation frameworks.

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 3 warrant the accuracy or completeness of the information or analysis contained in this report.

International Securities Services Association ISSA
c/o UBS Switzerland AG
EUR1 – EG2230, P.O. Box
CH-8098 Zurich, Switzerland
Contact +41 (0)44 239 91 94
issa@issanet.org

Table of Contents

1. Executive Summary

Significantly adverse consequences associated with cyber attacks are seen on a far too regular basis across many industries, services and infrastructure environments. This document provides an assessment of the threats and risks specific to Securities Servicers and explains why ISSA believes this threat is real and requires urgent and constant focus for those operating within this space.

While high profile cyber attacks within the financial services sector demonstrate that a primary motivation has been the theft of monies via payment mechanisms through the Payment Services sector, the Securities Services sector itself is a generator of considerable volumes and values of money movements, particularly through settlement of securities trades, income events and corporate actions.

Securities Services firms hold significant client data which include account details to which payments are made. Securities cash flow is known (e.g., dividend pay-dates) and publicized. The risk of fraudulent alteration of these account records knowing that payments will be made on set dates is a potential motivating factor for a cyber-attacker. The risk is further increased should a Securities Servicer provide services where payments/ cash movements are not expected or closely monitored in a time sensitive manner by the payment recipient.

Theft of securities may be considered less appealing to cyber attackers than a payment related fraud given the financial benefit requires the securities to be exchanged for monies (and will consequently be delayed, which can result in more time for the Securities Servicer to identify and stop the fraud). However, Free of Payment Deliveries of Securities transactions may occur off exchange and do not always have matching controls. An analysis of cyber attacks shows that attackers are prepared to be patient. Free of Payment Deliveries of Securities, where the security is an instrument which affords the holder a payout in a short time frame such as a maturing bond with a close maturity date are a particular transaction type that has higher threat levels.

In addition to theft of assets and cash, Securities Servicers may also be exposed to data theft. The books, records and databases held provide attackers with the opportunity to obtain data which include client investments, portfolio details, performance and strategy, relationship information and fee agreements. Data stolen by cyber attackers can lead to significant ransom demands together with material reputational damage. The cyber threat posed by nation states and organized crime is also increasing. Cyber space remains a preferred operational domain for a wide range of industrial espionage and a means for some nation states to support their economic policy objectives.[1] These threat actors, if successful, may remain resident on a securities servicer's information systems to obtain information for foreign policy objectives.

However, the ISSA Working Group believes that major cyber attacks driven by a desire to materially disrupt key infrastructure are the most material and impactful of the threats faced. Securities Servicers are the infrastructure of the Investment Sector and disruption to the Central Securities Depositories, globally and domestically significantly important financial services firms (including the major Global and Sub Custodians) together with the industry wide utilities (such as SWIFT) could have a major adverse effect on the flow of monies at a national and international level.

[1] See Foreign Economic Espionage in Cyberspace at: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

However, various frameworks exist to mitigate the above threats, and the key components of these are listed within this document. Securities Servicers will largely be required under local regulation to implement cyber security frameworks and ISSA notes that baseline standards such as ISO 27000 series, NIST Cybersecurity Framework and SWIFT's Customer Security Programme (CSP) exist to help benchmark Securities Servicers' cyber security policies and procedures. In the event of cyber attack, management must react rapidly to detect the attack, isolate the issue and assess the impact. This document sets out the key internal controls ISSA believes are appropriate and sets out the principles and objectives of these risk mitigants together with the parties that would be responsible as well as the anticipated results and outcomes of the controls.

While Securities Servicers clearly need to have robust cyber security frameworks, they also need to assess the risk to themselves of cyber attack on their clients, vendors and counterparties. Due diligence over the cyber risk management program and associated controls of these third parties is critical and ISSA believes that appropriate contractual obligations should be placed on third parties to meet the policy and standards of the Securities Servicer firms, which can include an attestation process by these third parties to provide their status in complying with these standards.

Securities Servicer firms should establish risk management processes that map the status of third parties' compliance obligations vs. the Securities Servicer firm's own risk assessment (such as AML rating of the country the third party resides in, the inherent risk with the service provided and transparency afforded). This may lead to additional countermeasures being implemented.

This document highlights the various cyber security frameworks that should be leveraged by Securities Servicers but goes further to recommend specific risk mitigation techniques across the firm, including internal controls and cyber security due diligence regarding clients and third-party service providers.

With continuing developments and reliance on changing technology (e.g. robotics, machine learning,, artificial intelligence, cloud data storage, cryptocurrencies and blockchain) impacting Securities Servicers, the cyber attack threat is likely to continue to increase and Securities Servicer firms must continue to invest in risk mitigation strategies and develop Securities Services specific collaborative and active intelligence networks.

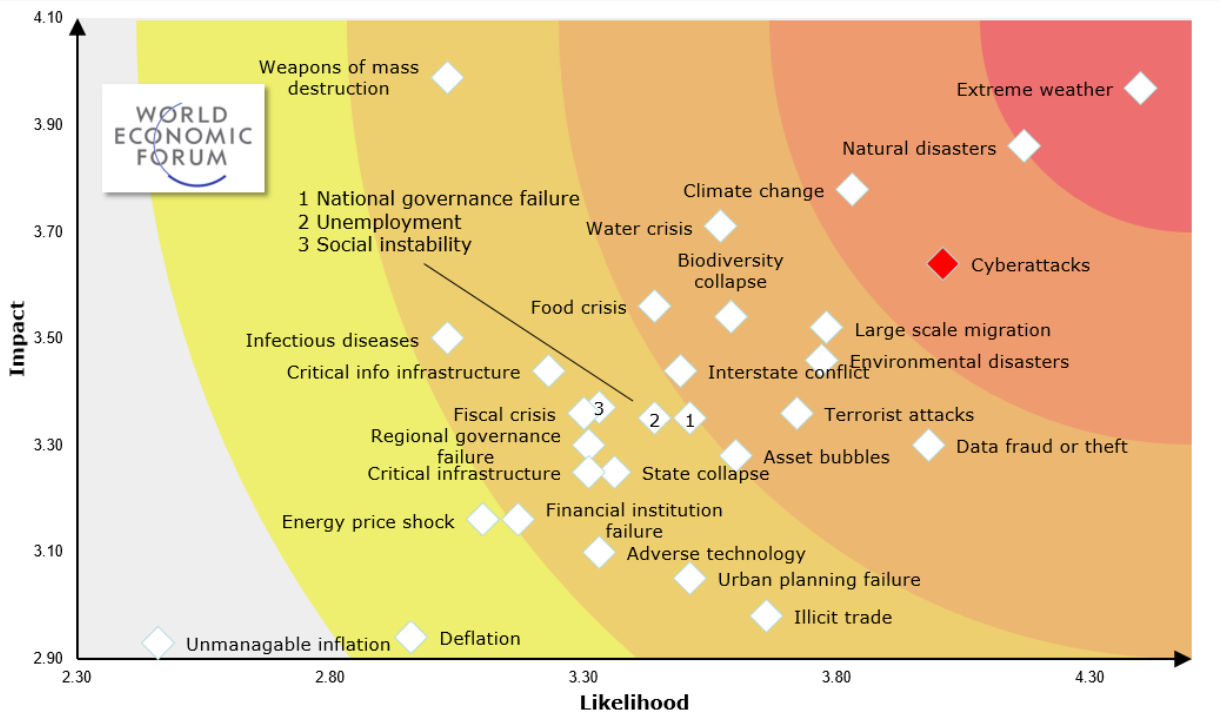
2. Threat Landscape

2.1 The Big Picture

In its *Global Risks Report* for 2018, the World Economic Forum (WEF) considered that cyber attacks are ranked third in their top 10 risks from a likelihood perspective and sixth in terms of impact.

The WEF comments that cyber security risks are growing in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years and incidents that would once have been considered extraordinary are more and more commonplace. The financial impact of cyber security breaches is rising and some of the largest costs in 2017 related to ransomware attacks.

Figure 1: Global Risk Perception



Source: WEF survey spanning 684 respondents which assessed [likelihood] and [impact] of each risk on a scale of 1 to 5 [very unlikely / minimal impact] to [very likely / catastrophic].

The WEF considers that the expanding use of cloud services and the Internet of Things (IoT) is likely to continue to attract an increase in cyber attacks as bad actors identify more targets.

2.2 Threat Types

The term 'cyber attack' is broad and can encompass many different types of malware, attack types and initial injection vectors, as outlined below.

2.2.1 Malware

Cyber attacks, at their very core, are built around software executables of varying flavors:

- **Virus:** A piece of malicious code that attaches itself to a program or file so that it can spread from one computer to another. Viruses travel by copying over a network via file sharing or infected e-mail attachments.
- **Worm**: A piece of malicious code that can spread without human interaction by using the system's normal transportation features.
- **Trojan:** A piece of malware that appears as a legitimate application but creates back-door access to the system when activated. Trojan malware does not propagate across the network.

2.2.2 Attack Types

These viruses, worms, trojans and other executable components are constructed into different attack types. Of note:

- **Ransomware:** A type of malicious software that prevents or limits users from accessing their system either by locking the system screen or encrypting files until a ransom is paid, e.g. WannaCry, NotPetya and BadRabbit.
- **Distributed Denial of Service (DDoS):** A type of cyber attack that uses systems' resources of compromised computers / devices to make an Internet service, site or application unavailable to its intended users**.**
- **Advanced Persistent Threats (APTs):** A set of structured continuous and sophisticated attacks that are used to compromise a targeted entity**.**

2.2.3 Initial Injection Vector

Cyber attacks are either targeted (where the intended victim is pre-identified) or untargeted:

Targeted Attacks

- **Spear Phishing** e-mail, e.g. targeted and personalized e-mail messages / social engineering that is finely tailored to the target.
- **Removable media drives or USB sticks** e.g. used in the Stuxnet Worm attack.
- **Insider** e.g. typically an insider is an employee of the company that has greater access to sensitive information, a better understanding of internal processes and knowledge of high-value targets and potential weaknesses in security.

Untargeted Attacks

- **Phishing** e-mail, e.g. *WannaCry*, ransomware attack that sent millions of malicious e-mails and infected hundreds of thousands of computers globally.
- **Web Site / Watering hole** attacks an infected website that is frequently used by potential victims, e.g. Central Bank or Financial Supervision Authority.
- **Adware malware** which presents unwanted advertisements to the user of a computer e.g. *Fireball Adware.*

For the securities market, targeted attacks, either APT, Ransomware and / or DDoS are considered highly relevant.

2.3 Threat Actors and Motivations

The different types of threat actors, and their underlying motivations, tend to fall into a handful of different types, as summarised by the table below.

	Funding Levels	Disruption Levels	Motivation
Nation States	High	High	• Political unrest • Economic disturbance • Espionage • Intellectual property • Financial gain
Organised Crime	Medium	Medium	• Financial gain • Intellectual property
Hactivists	Medium	Medium – High	• Reputation damage • Operational disruption • Social / political ideology
Malicious Insiders	N/A	Medium – High	• Revenge • Operational disruption • Intellectual property • Financial gain
Unwitting Insiders	N/A	Medium – High	N/A - accidental impact / disruption

Sources: Verizon 2017 Data Breach Investigations Report
IBM X-Force Threat Intelligence Index 2017
ENISA Threat Landscape Report 2017

Given the nature and makeup of the Securities Servicers sector and its concentration of very high value assets, its complexity with many integrated parts and its reliance on centralized critical functions and utilities - the ISSA Working Group focused on sophisticated attacks from threat actors that are likely motivated by financial gain, political gain or information theft.

Depending on the underlying motivation, the types of cyber attack and how they are constructed may differ – for example an APT attack may be used to steal assets or plant ransomware in a strategically important system whereas a DDoS attack maybe used to disable an internet-facing customer portal.

2.4 Phases of a Cyber Attack – the Kill Chain

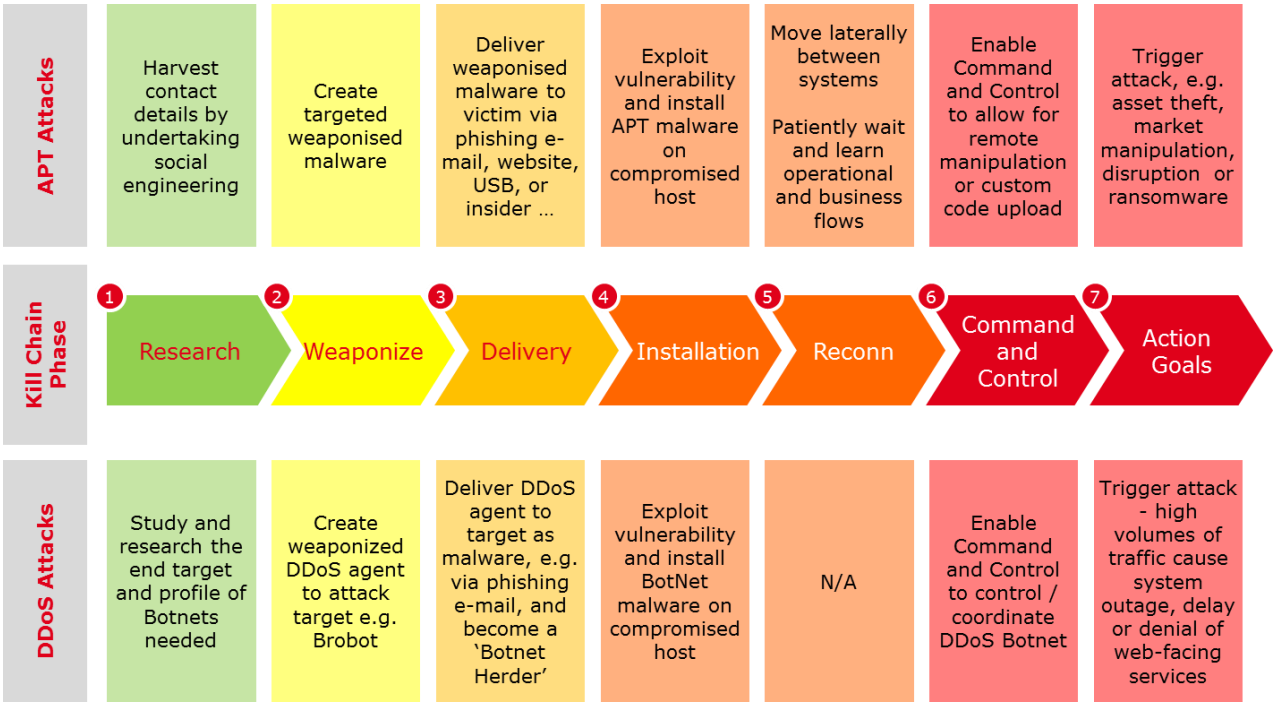
Cyber incidents can disrupt critical financial services and thereby undermine the security and confidence of the financial system. As network defenses have become stronger, the skills necessary to develop tools to circumvent these controls have become more sophisti-cated. The threat actors attacking the Securities Servicers sector are well-resourced, trained and adept at developing and launching intrusion campaigns known as Advanced Persistent Threats (APTs). APTs are a set of structured continuous and sophisticated attacks that are used to compromise a targeted entity. The threat actors conducting these APTs are attempting to compromise or extract information for economic, political and national security advancement. Given the amount of time and resources used to conduct these attacks, these threat actors are looking to remain undetected through the course of the APT campaign. The ultimate goal of the threat actor is to remain undetected through

the course of the APT campaign and continue to conduct additional campaigns within the targeted entity (see timings in next section).

The Lockheed Martin Cyber Kill Chain (illustrated below) is the series of steps that an adversary must conduct to successfully gain access to the entity. An organization's ability to disrupt the threat actor at any point in the Kill Chain not only stops the attack but it also allows for intelligence to be gained regarding the attack and provides insights into potential future attacks. Organizations should aim to disrupt the attacker as early in the Kill Chain as possible to enable a quick recovery.

To illustrate how the adversary follows the Kill Chain, the below outlines two example use cases for an APT and Distributed Denial of Service (DDoS) attack.

Figure 2: 'Kill Chains' for APT and DDoS Attacks



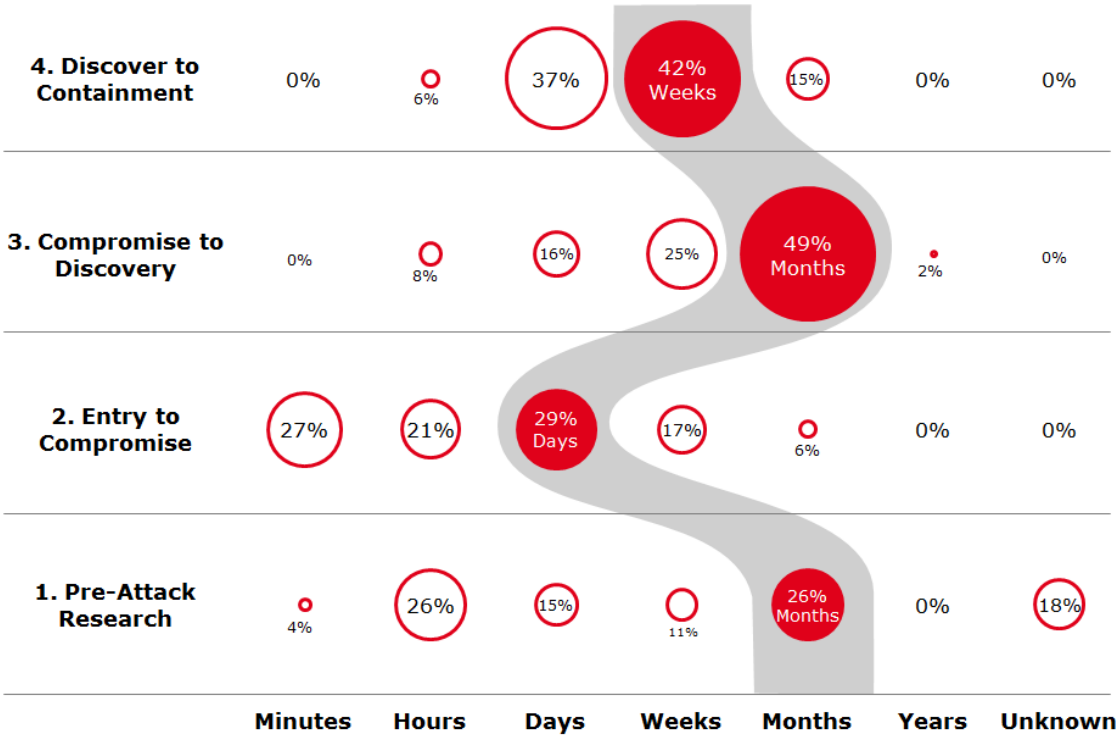
Source: Based on Lockhead Martin 'Kill Chain' Framework

In addition to each phase of the Kill Chain being distinct, each will have different timing characteristics before, during and after an attack.

2.5 Typical Timings Before, During and After a Cyber Attack

According to Verizon, threat actors can invest weeks or months on a targeted attack, as indicated by the graphic below.

Figure 3: Typical APT Timespans



Source: Verizon 2009 Data Breach Investigations Report

SWIFT Experience (see also Appendix 1)

This pattern of patience and heavy investment in reconnaissance is also borne by SWIFT's experience with the threat actors that have attacked organizations that use the SWIFT network.

After forensic examination following an attack, there is evidence that some threat actors can spend **many months** after initial compromise in reconnaissance, gathering information on the victim's systems, architecture and operational practices.

After they have gathered sufficient information, then the creation of fraudulent payments messages can take a matter of **minutes**.

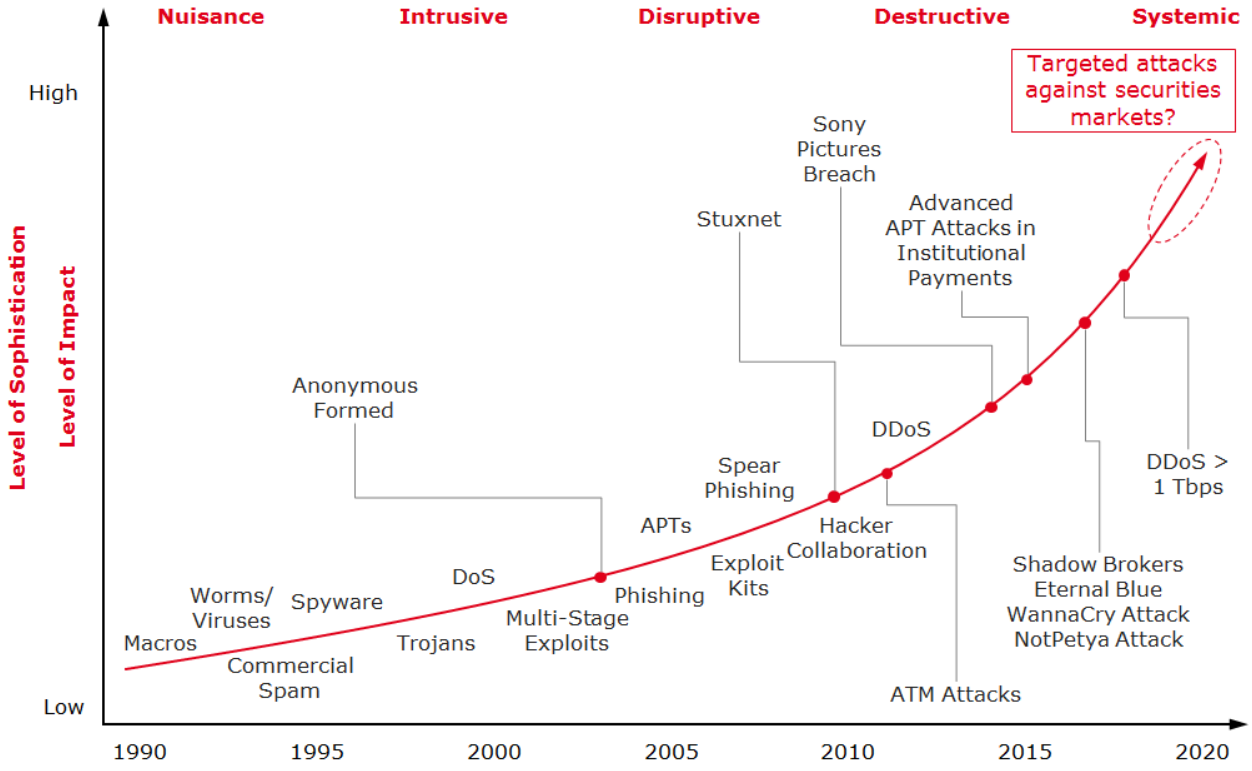
After the attack, if the victim can maximize the chances of funds recovery, they can identify anomalous behavior within a **few hours** and then recall or cancel the messages and/or freeze the end beneficiary account.

2.6 Evolution of Cyber Attacks

The cyber threat landscape continues to evolve and the attack surfaces open to the threat actors continue to change. With Advance Persistent Threat (APT) cyber attacks, virtually anybody could be a target and with Internet of Things (IoT) everything could be used as a DDoS weapon.

As the level of impact and the level of sophistication of attacks rise, there is risk that securities markets may be impacted.

Figure 4: Evolution of Cyber Attacks



Source: ISSA Working Group analysis

This report attempts to extrapolate this curve by identifying the susceptibility factors and specific risks for the securities market. It looks at the broad risk clusters and undertakes a comparative risk assessment which quantifies the level of systemic reach, the ease of execution and the possible impact.

3. Risk Assessment

3.1 Susceptibility Factors for Securities Services

Cyber attacks centered on the theft of assets via payment channels are currently the most pervasive type of asset theft, particularly as the threat actor would likely want to be able to receive monies in a bank account quickly. However, there are attributes and susceptibility factors within the securities servicing market which make a cyber attack relevant and a strong possibility.

While securities can be fraudulently moved and the ownership changed, the threat actor would still need to convert / sell the security in order to receive monies. This delay may be a deterrent. However, securities services include significant operational attributes and flows that may be attractive to a threat actor. In addition, securities servicer organizations hold significant amounts of highly confidential data, including their clients' holdings and transaction patterns and beneficial owner records which have value to a malicious party.

Key susceptibility factors that are specific to the securities market have been identified as follows:

Major Susceptibility Factors:

- Concentration of very high value assets
- Securities industry is complex with many entry points, moving parts and functions
- Predictable asset and money movement flows - maturities and dividend schedules
- Reliance on centralized critical functions, such as matching engines, CSDs for settlement, CCPs for clearing and Trade Repositories for regulatory reporting

Secondary Susceptibility Factors:

- Use of omnibus vs. segregated accounting can obscure end beneficiary details in part of the chain and create challenges in the identification and timely detection of fraudulent positions by all layers in the custody chain
- Contrasted use of automation and Straight Through Processing (STP) in some areas of transaction processing and automation reconciliation versus reliance on manual handling
- Concentration of asset flows with high values, with bulk asset movements
- Reliance on data, from a small number of vendors, such as pricing and Standing Settlement Instructions (SSIs)
- Reliance on a small number of outsourced service providers, some of which have low-cost locations in locations susceptible to cyberattack
- Need for internal staff to meet daily operational deadlines
- Use of High Frequency Trading (HFT) algorithms to automatically establish asset pricing and trading

3.2 Risk Clusters

Within the securities value chain, the ISSA Working Group identified **four broad clusters** of cyber risk which may be either internally or externally introduced:

1. **Cluster A - Utility Disruption / Ransom**: The risk of systemic market disruption, destruction or ransom targeted at market infrastructure with resultant market liquidity issues due to an APT and/or DDoS attack. If targeting a central utility, that typically would have stronger defences than an average market participant, the attack may be more difficult to undertake, but the reach could be wide and the impact could be very high to the market. This could include sabotage from an insider.
2. **Cluster B - Asset Theft**: The risk of asset theft and financial loss from manipulated records for a specific organization from a coordinated APT attack. Depending on the targeted organization, the impact would be localized.
3. **Cluster C - Information Theft**: The risk of information theft of sensitive intellectual property that could give competitive advantage from a coordinated APT attack and could cause reputational damage, rather than direct financial loss. Depending on the targeted organization, the impact would be localized.
4. **Cluster D - Market Manipulation**: The risk of manipulation of pricing and / or news feeds from a coordinated APT attack. Stock prices would adjust automatically and buy/sell orders would be fulfilled automatically, resulting in potential financial gain if the attackers were stock holders.

3.3 Comparative Risk Assessment

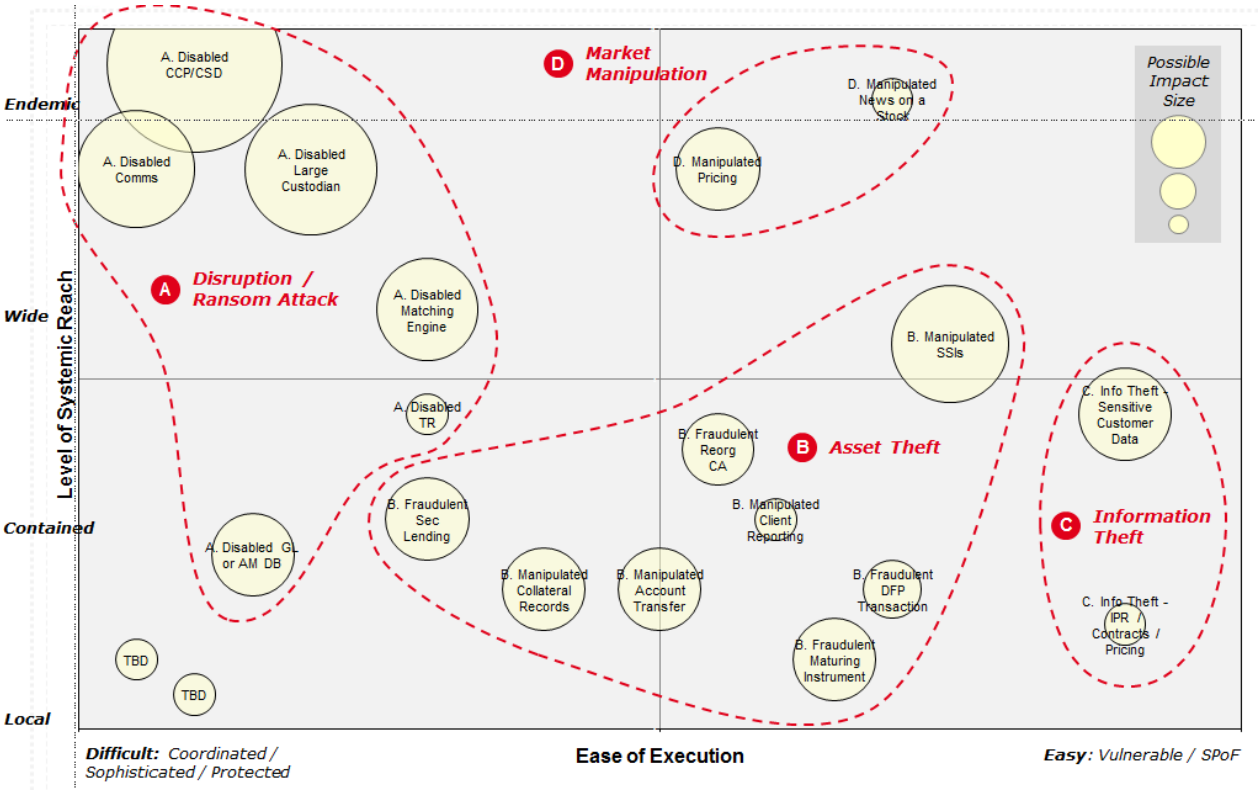
The ISSA Working Group reviewed a specific (and certainly non-exhaustive) list of key securities servicer functions / activities and determined how they map to the broad risk clusters, as outlined above.

For each securities servicer function, the ISSA Working Group assessed the likely impact if that securities servicer function had been breached from a cyber attack. The group estimated the relative risks across three axis:

- **The level of systemic reach**: From 'Local' and 'Confined', through 'Widespread' to 'Endemic'. Represented on the Y-axis
- **The ease of execution** of the attack by the threat actors: From 'Difficult' (well protected, attacks would need to be coordinated and sophisticated) through to 'Easy' (vulnerable, not well protected, single point of failure). Represented on the X-axis
- **The possible size of the impact**: Disruption / ransomware ('minor' to 'market paralysis'). Asset theft and market manipulation ('Millions EUR' to 'Billions EUR'). Information theft (where reputation damage is 'minor' through to 'non-recoverable'). Represented as the size of the 'bubble'

The summary output of the risk assessment is shown in the diagram below and described in the next section.

Figure 5: Key Cyber Risks in the Securities Value Chain



Source: ISSA Working Group analysis

3.3.1 Disruption / Ransom Attack

The motive for a disruption / ransom attack is either to cause economic disturbance for the entity and / or market (e.g. liquidity challenges). Within securities services, examples could include:

- Central Counterparty (CCP) for clearing, Central Securities Depository (CSD) for settlement or Trade Repository (TR) for regulatory reporting
- Global custodian
- Major service provider
- Central matching engine
- Inter-bank messaging service, such as SWIFT
- General Ledger, Asset Master or Custody Record database of a specific market participant

The WEF report notes that some of the largest costs in 2017 related to ransomware which at the time of writing is considered a growing form of malware that locks targets out of their data and demands a ransom in return for restoring access. Recent examples (WannaCry, Petya/NotPetya and BadRabbit) were financially successful for the threat actors, but were *untargeted* relying on unpatched vulnerabilities. Despite this, these attacks impacted critical infrastructure in some countries and should serve as a warning to securities servicers.

Roles Performed by Securities Custody Service Participants

Global / Sub Custodians are responsible for holding their client's (e.g. asset owners) global/domestic securities assets off balance-sheet on a custody record that reflects the client's ownership interests in these assets.

The Global / Sub Custodian holds securities accounts with Central Securities Depositories (CSDs) and the client's ownership interests in the assets are held in the record of the CSD.

These holdings may have differing account conventions (e.g. Global Custodian name for account of client; Global Custodian Nominee or client's own name).

The Global / Sub Custodian's clients (asset owners) or their delegated parties (e.g. asset managers) instruct the Global Custodian to settle securities trades (move securities positions simultaneously against payment or free of payment).

The Global / Sub Custodian instructs the CSD to perform the settlement, moving the record of the ownership interest of the asset to the new asset owner's custodian relationship.

The settlement activity will also result in the Global / Sub Custodian moving cash to the required cash account with the respective Bank / Central Bank. Settlement activity (both securities & cash) is performed throughout the global day with multiple intraday deadlines.

Certain large **Global Custodians** service trillions of EUR / USD of assets and settle billions of EUR / USD of securities trades per day. The risk exists that a cyber attack may disable one or more of the Global / Sub Custodian's technology platforms which may include:

- Custody record system
- Securities movement system
- Corporate action system
- Dividend / income system
- Cash posting system
- Credit control
- Sanction screening application

Failure to perform securities servicing obligations may lead to settlement and FX losses for the custodian and leave clients short of securities and cash. This may lead to significant liquidity shortages and disrupt cash flows for the overall market. Typically, within a market, the **clearing and settlement** of a trade is a utility function performed by just one (or in some cases two or three) entities. Therefore, the disruption of a **CCP or CSD** could lead to failed clearing or failed settlement for the entire domestic market, which could in turn significantly stress the market's liquidity.

As a **messaging utility**, SWIFT serves the entire financial services industry. For securities, it provides standardized messages to move securities, instruct on corporate actions, instruct on FX and to provide confirmations and statements between Securities Servicers and their clients. As a result, Securities Servicers have developed sophisticated systems to enable highly efficient Straight Through Processing (STP). A major disruption to a messaging utility would significantly stress the market's liquidity.

A **matching engine** is a service that enables both sides of the securities trade to 'match' key information associated with the transaction and its settlement instructions. Depending on the vendor, there are 'central' matching engines and 'local' matching engines. Although disruption to a specific matching engine would cause trades to fail, the market is not reliant on one solution provider.

In all disruption cases, the market would revert to its well-rehearsed backup contingency plans. These alternative plans would largely rely on manual communications, where custody and settlement activities would be prioritized.

In terms of likelihood, the ISSA Working Group determined that utilities and market infrastructures, which are under significant regulatory oversight and scrutiny, would be typically well defended, making attacks difficult to execute successfully.

3.3.2 Asset Theft

The securities market may be particularly susceptible as Securities Servicers move significant values of transactions daily, particularly securities delivery / receipt versus payment, large bond maturity payments, corporate actions, dividend and income payments, tri-party repo payments and deposits. The motive for asset theft is simply financial gain.

Specifically, asset theft would include attacks that manipulate or create fraudulent records or transactions somewhere along the securities value chain, for example:

- Fraudulent 'Delivery Free of Payment' (DFP) Transaction – see call out box.
- Manipulated Standing Settlement Instructions – see call out box.
- Manipulated Client Reporting or Statement of Holdings.
- Manipulated Collateral Records, for example where securities could be illicitly borrowed on loan against artificial collateral as part of a Securities Lending transaction.
- Fraudulent Account Transfer Records – where the asset owner's portfolio is moved from one custodian to another. This account transfer is a movement of multiple securities positions 'free of payment'. The account transfer or 'out-conversion' is performed as a high touch operation with close oversight by the asset owner, asset manager and the delivering and receiving custodian.

Use Case: Fraudulent 'Delivery Free of Payment' (DFP) Transaction

Asset owners or their Investment Managers can instruct the delivery of securities from their portfolio and transfer ownership to another party without an exchange of monies via a 'Delivery Free of Payment' transaction.

For example, DFP transactions may relate to a bond security with a close maturity date.

DFP transactions occur on an off-exchange OTC basis and are not always subject to a formal matching process.

The risk exists that a malicious party could introduce a fraudulent instruction through either an industry messaging utility or via a custodian's client-facing electronic portal and instruct the movement of securities from the securities account to an account that the fraudster has opened elsewhere.

Use Case: Manipulated Standing Settlement Instructions

Asset owners or their Investment Managers direct their Custodian as to where they require funds to be paid to and securities moved.

These details, including the bank and account details, are recorded as 'Standing Settlement Instructions'.

The risk exists that the cyber fraudster obtains access to the Custodian's database of client Standing Settlement Instructions and changes the account to be paid / securities moved to an account the fraudster has access to.

In asset theft cases, the impact would be confined to immediate parties involved without risk of contagion to the overall market. Arguably the only exception is Standing Settlement Instructions, where specific vendors provide SSIs as a centralized service.

In terms of likelihood, the ISSA Working Group determined that asset theft would be dependent on the defences adopted by the local participants, who would vary depending on the size and maturity of the individual participant (see section 4) but, in general, these participants may be easier to penetrate than market infrastructures.

3.3.3 Information Theft

The motive for information theft may be for a competitive advantage over a rival organization, to potentially cause reputational damage if the information is purposefully leaked or to further a nation state's economic policy.

Within the securities market, this could include the theft of:

- **Intellectual property**, such as customer contracts, pricing schedules, product or service information
- **Sensitive customer data**, such as customer positions, holdings, statements and personal contact details

However, in a recent case[2], information theft was used for financial gain.

In 2017, in the US, the Securities and Exchange Commission (SEC) revealed that its EDGAR database was subject to a cyberattack in the prior year.

EDGAR is used to store US corporate filings, company financial statements and sensitive information about mergers and acquisitions.

According to the SEC Press Release, the attack exploited a software vulnerability, stole undisclosed information which then '*may have provided the basis for illicit gain through trading*'.

3.3.4 Market Manipulation

The motive for market manipulation is financial gain, whereby the threat actor seeks to artificially manipulate the price of an asset. Within the securities market, this could include:

[2] SEC Press Release, 2017-170, 20 Sept 2017

- Multiple, simultaneous buy and sell orders on a stock, where the increased trading activity artificially increases the stock's price.
- Simultaneous rumors or 'fake news' on a stock, by illicitly manipulating multiple newswires or news sources.
- Simultaneous manipulated intraday pricing feeds from established financial data vendors.
- Manipulation of the terms of a complex reorganization or Corporate Action, such as a merger, to artificially impact its attractiveness to the market.

If a threat actor is able to penetrate and compromise a pricing feed vendor(s) or newswire(s) and affect the price of a specific stock, then this information would allow the threat actor to buy or sell at the artificial price. As the system or network compromise is physically far from the financial transaction, this type of illicit trade could be difficult to trace.

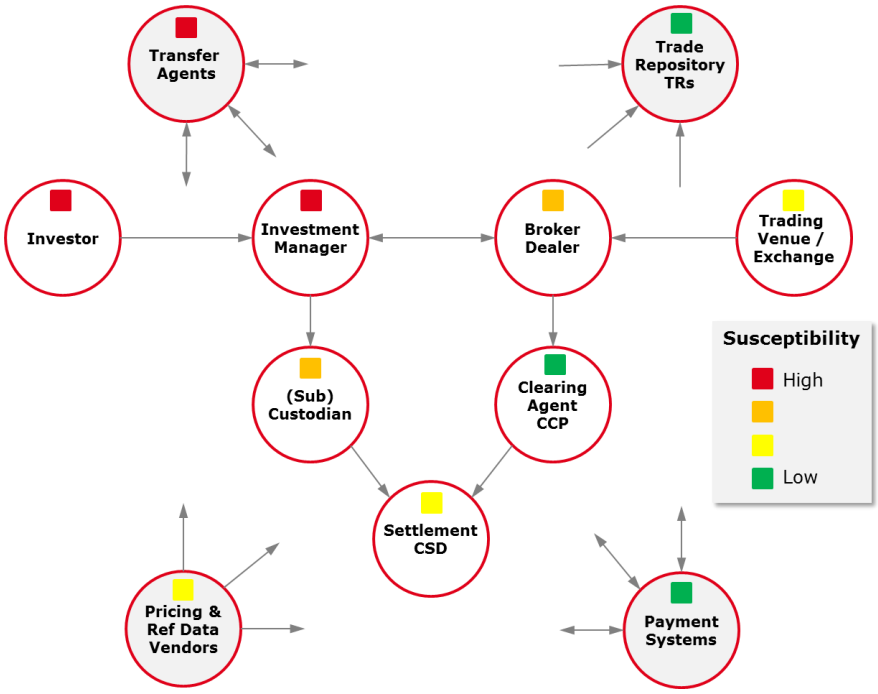
Similar to the 'Information Theft' example above, in a formal statement from the SEC, the SEC Division of Enforcement states it '*has investigated and filed cases against individuals who [SEC] allege placed fake SEC filings on the EDGAR system in an effort to profit from the resulting market movements*'[3].

[3] SEC Statement on Cybersecurity, 20 Sept 2017

4. Susceptibility of Securities Participants

The securities value chain is complex with many moving parts. It comprises many different participant types that perform many different functions and services. As a gross simplification, the overall securities custody value chain is shown below:

Figure 6: Susceptibility within the Securities Custody Value Chain



Source: ISSA Working Group analysis

Aside from assessing the range of possible cyber risks, the ISSA's Working Group also tried to gauge the perceived level of relative susceptibility of various participant types within the securities value chain based on several factors - this is indicated as the colored overlay.

The Working Group agreed that the degree of cyber perceived susceptibility will depend on many factors, including the jurisdiction's overall level of cyber maturity, but in general the factors may include:

- **Organization size and staffing levels** which would influence the extent of in-house cyber security skills.
- **Degree of automation and reconciliation** versus manual processing within the participant type.
- Whether the participant is reliant on **bilateral coordination** and handshaking between two trading partners versus unilateral action from a single player.
- Presence of a **central regulator**, overseer or supervisor, especially if acting as a central utility.

As a result, the Working Group found that all participant types are susceptible and must be vigilant in increasing their cyber security risk management capabilities. Smaller firms tend to be more at risk but fragmented technology architecture, over reliance on aged legacy systems and manual processes is evident across the industry – both in small and larger firms. Some Investment / Asset Managers, Investors and Transfer Agents have been highlighted as being more susceptible than other segments but size is not always a reliable indicator of sophistication and resilience.

5. Existing Regulations and Frameworks

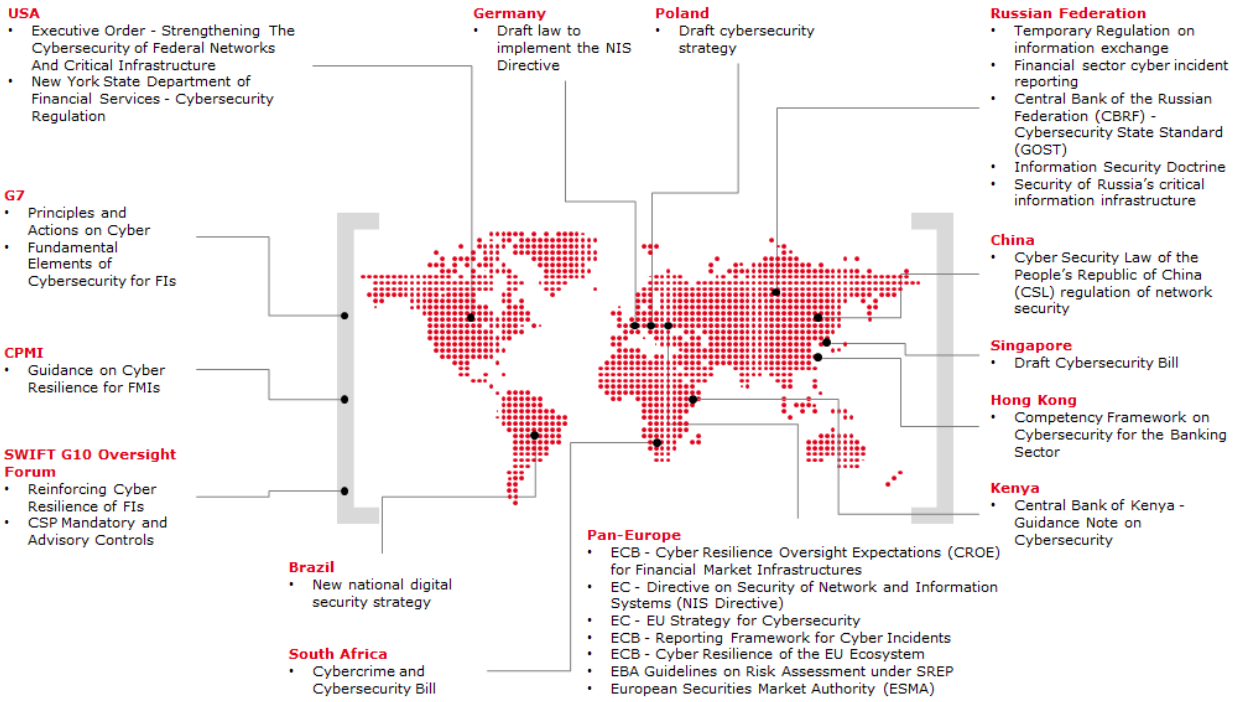
5.1 Existing Regulations and Policies

Globally, the introduction of new legislation and guidelines that impact cyber security is increasing. The G20 Finance Ministers and Central Bank Governors noted that the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermining the security and confidence and endanger financial stability. The Financial Stability Board (FSB) has requested, as a first step, to perform a stocktake of existing relevant released guidance and supervisory practices. This resulted in the FSB paper entitled '*Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*' (October 2017).

The graphic below, which is not intended to be exhaustive, shows the diverse nature of policies and regulations which are either already in place, or are being implemented, that help mitigate cyber risks.

These policies and regulations are, by their very nature, jurisdictional and mandatory, and many organisations would have to meet to a patchwork of different regulations in order to fully comply.

Figure 7: Policies / Regulations that Can Help Mitigate the Cyber Risks



Source: Financial Stability Board: Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, 2017

However, aside from policy and regulations, there are existing frameworks and guidelines that can also help defend against cyber attacks.

5.2 Existing Frameworks, Guidelines and Standards

Aside from jurisdictional mandatory policies and / or regulations, there are a number of existing cyber-related advisory frameworks / guidelines that can be seen as market 'best practice'. Examples of these frameworks and guidelines are found in the table below:

Label	Title	Description	Market	Published
BCBS	Basel Committee on Banking Supervision	Risk Management Principles for Electronic Banking	E-banking	2003
CPMI-IOSCO	Committee on Payments and Market Infrastructures / International Organization of Securities Commissions	Guidance on cyber resilience for financial market infrastructures (including two hour recovery)	FMIs	2016
G7 CEG	G7 Cyber Expert Group	G7 Fundamental Elements for Cybersecurity	All	2016
OECD	Organisation for Economic Co-Operation and Development	Recommendation of the Council on the Protection of Critical Information Infrastructures	FMIs	2008
OECD	Organisation for Economic Co-Operation and Development	Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity	All	2015
ISACA COBIT	Information Systems Audit and Control Association	Control Objectives for Information and Related Technology	All	1996
ISO IEC	ISO	ISO 27000 family of standards	All	2013
NIST	US National Institute of Standards and Technology	Framework for Improving Critical Infrastructure Cybersecurity	All	2018
FFIEC	Federal Financial Institutions Examination Council	FFIEC Information Security Handbook	Banks	2016

To varying degrees, these different frameworks cover some or all aspects of the following:

- Risk Management
- Governance and Roles
- Controls, Measures and Policies
- Review / Audits
- Information Security Confidentiality / Integrity / Availability / Encryption
- Threat Monitoring and Detection
- Vulnerability Management
- Asset Management
- Access Management
- Recovery and BCP
- Reporting, Notification and Information Sharing
- Training and Awareness
- Third Parties and Outsourcing

To illustrate, key components of the widely-used NIST Cybersecurity Framework are depicted below:

Figure 8: NIST Cyber Security Framework

Source: NIST Cybersecurity Framework

6. Recommended Risk Mitigation Practices / Internal Controls

Given the threat landscape, the evolving regulatory landscape, the introduction of new technologies (e.g. cloud, blockchain) and the business operational risks, the approach to managing cyber security risks is one that should be layered through the people, processes and technologies of the organization. The foundation of any cyber security risk management program should be built on a cyber security framework. This framework will identify those control areas for which the organization will define policies and standards to protect their business operations.

Cyber security risk management is the process of identifying vulnerabilities and threats to information resources and business operations and deciding what countermeasures, if any, to take in order to reduce risks to an acceptable level. Effective risk management begins with a clear understanding of the organization's appetite for risk. This drives all risk management efforts and impacts future investments in this space.

The risk programs and services outlined in the following subsections define those risk mitigation efforts that will address those risks identified in Section 3 of this document. It is not meant to define a comprehensive cyber security risk management strategy.

Securities Servicer organizations should look to implement comprehensive cyber security programs based on their defined risk profile and in line with their supervisory / regulatory obligations. The maturity of these programs may differ based on the type, size and complexity of the organization's business operations, including but not limited to their customers and counterparties, markets and products traded and services as well as the access provided to trading venues and other servicer participants.

6.1 Threat Intelligence and Information Sharing

Principle & Objective
A threat intelligence capability should be established which supports an intelligence cycle together with analytical tools. The primary objective of a threat intelligence program is to provide information and situational awareness about past and ongoing attacks while providing insights and predictive information on potential future attacks. Threat intelligence supports risk-related decision planning and facilitation of corrective actions.

The intelligence cycle should collect threat intelligence and supporting details from internal technical infrastructure (e.g. Security Information and Event Management systems [SIEM], device logs, intrusion detection systems, gateways, proxies and other meaningful sources).

Threat intelligence should also be collected from external sources (e.g., trusted intelligence providers or advisors, government agencies or national Computer Emergency Response Teams (CERTs), publicly available information and collaborative threat intelligence groups).

Threat information gathered should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information on geopolitical developments that may trigger cyber attacks on any entity within the company's ecosystem. Threat intelligence may also be actionable and require an organization to evaluate its process- and technology-based controls and implement countermeasures, if necessary, to limit the exposure to the threat.

This information should be regularly assessed and reviewed by skilled analysts to produce requirement-driven threat intelligence as an early warning system to identify emerging

threats which may target the company. Analysts should analyze past attacks in order to identify techniques used by the attackers to maintain control of compromised systems.

Involved Roles & Owners
The intelligence cycle should be embedded within the Company's Security Organisation. Intelligence Analysts may share findings with the intelligence community through:

- Country or regional Computer Emergency Response Teams (CERTs), e.g. organizations such as FIRST, US-CERT, CERT-EU, Asia Pacific CERT (APCERT)
- Information Sharing and Analysis Centers (ISACs), e.g. organizations such as FS-ISAC, FSIE, FI-ISAC
- Industry groups, e.g. organizations such as Cyber Defense Alliance (CDA), Financial Systems Analysis and Resilience Center (FSARC), Cyber Coalition
- or simply peer-to-peer via e-mail distribution lists within 'trusted groups'.

Specialized security analysts should be assigned to this threat intelligence team, while the owner of the function itself is the responsibility of the Chief Security Officer (CSO) or Chief Information Security Officer (CISO).

Expected Results
Threat intelligence should provide Securities Servicers organizations with insights into the current threat landscape. Threat Intelligence may allow for entities with the Securities Servicing markets (e.g. CCP, CSD, Custodians) to identify potential cyber attacks that could lead to a significant disruption of the financial markets. Identified threats that target custody records, standing settlement instructions, securities movement, cash posting and credit control systems should receive additional scrutiny. Cyber incidents affecting these systems may lead to liquidity shortages and disrupt cash flows within the Securities Servicing sector.

6.2 Vulnerability / Patch Management

Principle & Objective
Vulnerability Management is the continuous process of identification, classification, remediation and mitigation of system vulnerabilities. Software patches are often used to remediate Information System vulnerabilities, therefore the terms vulnerability and patch management are often used interchangeably. Vulnerability Management begins with the identification of Information System weaknesses through a software scanner. In order to effectively identify these weaknesses, the software scanner should have access to all network segments. For network segments, where the software scanner is not permitted, a risk analysis should be conducted and reasonable safeguards should be provided. The frequency of the identification of software vulnerabilities (i.e. vulnerability scanning) should be determined by:

- The organization's risk appetite
- Supervisory rules, rules interpretation, and notices
- The threat landscape

Software vulnerability scanning may be authenticated or unauthenticated. The method of scanning chosen by the organization should be evaluated after considering the risks associated with each method and their network environment.

Once the software weaknesses have been identified, the organization should classify the weaknesses. Classification of these weaknesses may be the result of the several factors including but not limited to:

- Location of the vulnerability within the computing environment (e.g. internal vs external network)
- Ease of vulnerability exploit
- Business impact of the software weakness
- Other organizational process and technical safeguards

The classification of software weaknesses should lead to a remediation schedule that is determined by the organization's risk appetite. Remediation may require the application of a software patch, a newer version of the software, or the application of compensating controls.

Given the number of cyber incidents that have been the result of missing patches and system vulnerabilities, organizations should be vigilant in their Vulnerability Management program.

Information Systems may also be vulnerable because the software / hardware manufacturer no longer supports the application or system. These systems are known as 'End of Life' or 'End of Support' systems. While in some instances, the manufacturer may offer extended support for a limited timeframe, software patches are normally provided only for the highest of vulnerabilities and for a timeframe adequate for the organization to transition off the Information System. Securities Servicers should understand their exposure to these systems and determine what, if any, mitigating controls may exist to manage this risk. Organizations should also identify those actions that may be required to transition off these systems. Vulnerability Management is markedly enhanced by an accurate information system inventory. IT Asset Management is the process of gathering and maintaining hardware, software, and ownership information on information systems through the introduction to the retirement of these systems within the business's computing environment. Without a reliable IT Asset Management program, information systems may fall outside of the vulnerability scanning process and subsequently be left unpatched. Since other cyber security risk management programs (e.g., Identity and Access Management, Risk Assessments) rely on the accuracy of this information, organizations should dedicate sufficient resources to ensuring the accuracy of this information.

Involved Roles & Owners
There are several roles and owners in the Vulnerability Management program. The implementation of remediation actions (e.g. software patches, configuration changes) are normally the responsibility of the IT department, while the organization's business managers are accountable for providing times when remediation activities may take place. The Risk organization is responsible for the measurement and reporting of Vulnerability Management activities including the development of Key Performance / Risk Indicators (KPIs / KRIs) sufficient to inform the organization of the program effectiveness.

Expected Results
Given the number of cyber incidents that stem for the failure to patch Information Systems, a strong Vulnerability / Patch Management program is essential in managing the business's risk of disruption. Information Systems that provide critical securities servicing operations (e.g. custody records, standing settlement instructions, securities movement, credit control) should have stronger focus to ensure that vulnerabilities are managed for these systems.

6.3 Penetration Testing

Principle & Objective
While Vulnerability Management identifies known software weaknesses on Information Systems, penetration testing identifies systems misconfigurations and software design weaknesses (e.g. buffer overflows, code injections) that may exist within an Information System. A Penetration Test (also known as a 'Pen Test') mimics real-world attacks to identify methods for circumventing the security features of an application, system or network. It often involves launching real attacks on systems and data using tactics, techniques and procedures (TTPs) commonly used by attackers. Penetration testing can be useful for determining:

- How well the system tolerates threat actor attack patterns.
- The level of attack sophistication an attacker required to compromise the system.
- Additional countermeasures needed to mitigate threats against the system.

Given the potential impact of a Penetration Test to the operation of the Information System, it is recommended that organizations utilize experienced risk assessors to conduct these tests. Penetration testing should be performed only after careful consideration, notification and planning.

Involved Roles & Owners
The roles of the Penetration Testing program may be split between those executing the test and those individuals responsible for the remediation of identified risks. For appropriate segregation of duties, those individuals / groups that are responsible for the implementation and maintenance of the Information System should be separate from the individuals / groups that are responsible for the test execution. The implementation of remediation actions are normally the responsibility of the IT department. The business managers are accountable for determining when a penetration test may be conducted. The Penetration Testing assessors should be comprised of a team separate from that which implements and / or maintains the Information System and have demonstrable expertise to conduct these tests. Assessors may be internal or external to the organization.

Expected Results
Given the number of cyber incidents that stem from the failure to manage system vulnerabilities and poor software design, a strong Penetration Testing program is essential in managing the business risk of disruption. The organization should determine a risk ranking for those Information Systems (e.g. custody records, securities movement) based on the system's support of business operations and develop a schedule for the frequency of these tests. Supervisory guidance and rules may apply for this testing. Therefore, their requirements should also be considered when developing the frequency schedule.

6.4 Security Architecture

Principle & Objective
Security Architecture is a detailed description of all aspects of an Information System that relate to security along with the set of principles to guide the design. Security Architecture includes but is not limited to:

- Network Segregation
- Security Baselines
- Authentication Mechanisms

Network Segregation allows for systems with different security requirements and / or operational environments to be physically or logically separated from other Information Systems on the network. The most common implementation of network segregation is the

organization's demilitarized zone (DMZ) environment. This environment is normally used to provide services to an organization's external clients and stakeholders.

Also known as 'trust zones', network segmentation also provides an additional security benefit of network isolation which may be used in troubleshooting or, in the event of an incident, may be used to limit the exposure to certain network segments. Network boundaries may be implemented through the use of routers, firewalls or gateways. They may also be set through the use of software (e.g. virtualization).

Security Baselines are a set of specific configurations for an Information System that are designed to limit the exposure of the system to cyber threats. Security Baselines may be set by the software / hardware manufacturer, the organization's information security group or a combination of the manufacturer and the organization's information security group. In order to ensure that these minimum controls are always set, the IT organization, together with Information Security, may create a secure build (i.e. a process designed to consistently apply certain controls to an Information System upon installation). Security Baselines may differ based on where the Information System resides on the organization's network (e.g. internal, Internet-facing).

Authentication Mechanisms are used to validate the user of the Information System. Authentication may be:

- Single-factor Authentication
- Strong Authentication
- Multi-factor Authentication

Authentication methods should be selected based on the information and services that are provided. The Federal Financial Institutions Examination Council (FFIEC) provides guidance on the authentication of critical Internet-facing services in its Authentication in an Internet-Banking Environment[4] guidance. While the guidance focuses on Internet Banking, it serves as a great example of when stronger authentication measures than username / password may be applied.

Where possible, Security Architecture should be designed prior to the implementation of the Information System or service within the production network environment. Applications may be available to measure the adherence to the security architecture (e.g. baselines) and should be considered for use by the organization.

Involved Roles & Owners
Security Architecture should be developed by the Information Security organization with input from the appropriate IT organization that developed the Information System. The implementation of the Security Architecture design elements is the responsibility of the IT organization. The second line of defense organization is responsible for measuring and reporting adherence to the Security Architecture through the development of Key Risk and Performance Indicators together with ongoing risk assessments.

Expected Results
The design, implementation and monitoring of the Security Architecture of an Information System mitigates the risk of business disruptions due to configuration weaknesses or the lack of consistent application of security controls. Security Architecture should be considered for those systems that provide critical services for the Securities Servicer and may include those systems that provide or hold custody records, standing settlement instructions, securities movements, record keeping and credit limits. A Security Architecture may,

[4] See FFIEC guidance on Authentication in an Internet Banking Environment at: https://www.ffiec.gov/pdf/authentication_guidance.pdf

in some instances, provide mitigating controls for asset theft (e.g. manipulated client reporting or statement of holdings). The risks of information theft of intellectual property and sensitive customer data are also mitigated through this program.

6.5 Identity and Access Management (IAM)

Principle & Objective
Identity and Access Management is the process of limiting access to authorized users based on what is required for their job responsibilities and to maintain this access from the time of access creation to the point in time access is no longer required. Key activities for IAM include account creation, user transfer, user certification and user termination.

This service also includes the management of Privileged Access and shared accounts to access Information Systems. These account types may be used to make unauthorized changes to the Information System or data and/or prevent accountability for these changes.

IAM may be simplified through the application of role-based access. Role-based access brings together groups of individuals with similar access needs and provides access permissions to the user group. Role-based access mitigates the risk of overprovisioning user access. Role-based access control also provides consistency in the provisioning of access to business groups.

In order to simplify the implementation of certain IAM activities, applications may be provided to automate the Identity and Access Management program and should be strongly considered when applicable.

Involved Roles & Owners
While the configuration and implementation of user- and role-based access is the responsibility of the IT department, the business managers should validate the access provided to the user (e.g. user certification). In addition to the periodic review of user access, the business managers should also review and validate the roles created for their area's usage. The Risk organization is responsible for developing KRIs and KPIs that may be used to measure the effectiveness of the program.

Expected Results
An Identity and Access Management program will institute preventative and detective controls that may limit the ability of an adversary to disrupt business operations. Securities Servicers should ensure that these controls are in place for systems that provide critical services which may include but are not limited to:

- Custody Records
- Securities Movements
- Standing Settlement Instructions
- Cash Posting
- Credit Control
- Sanctions Screening
- Reconciliation Systems

The ability to effectively manage user access may also limit Asset Theft by limiting the ability of an adversary to manipulate Client Reporting.

6.6 Intrusion Protection Management

Principle & Objective
Intrusion Protection Management is a defense-in-depth approach which is comprised of system tools and processes used to detect unauthorized access to an Information System. Information Systems that are commonly used to identify intrusions include but are not limited to:

- Network- and Host-based Intrusion Detection and Protection Systems,
- Anti-virus / Anti-malware

Intrusion Detection Systems may be host-based or network-based. Host-based intrusion detection systems are software-based solutions that reside on the Information System for which monitoring is being applied. Network-based intrusion detection systems are hardware-based solutions that sit in the line of network traffic to monitor for anomalous or malicious activity. There are two primary techniques for intrusion monitoring. Anomaly-based network monitoring is the process of comparing known good or normal network activity against observed events to identify significant deviations. An intrusion detection system using anomaly-based detection has profiles that may represent the normal behavior of users, hosts, network connections or applications. Profiles are developed by monitoring the characteristics of typical activity over a period of time. Profiles can be developed for many behavioral attributes, such as the number of web pages visited by a user, the number of failed login attempts for a host and the level of processor usage for a host in a given period of time: In some cases, profiles could be used to alert on potential account take-over or other fraudulent behavior.

The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. For example, identifying when a computer becomes infected with a new type of malware. The malware could consume the computer's processing resources, send large numbers of e-mails, initiate large numbers of network connections and perform other behavior that would be significantly different from the established profiles for the computer. This change may initiate an alert for a security operations analyst to review.

Signature-based Intrusion Detection Systems are effective at identifying known cyber attacks. Similar to anti-virus software, signature-based monitoring relies on the receipt of signature updates to continue to be effective. This monitoring type is only as effective as the organization's database of signatures. Signature-based Intrusion Detection Systems monitor attacks by looking for specific patterns or known malware behavior.

Anti-virus / anti-malware use signature-based techniques to detect patterns of malicious behavior and require an up-to-date database of signatures. In most cases, the signature updates will be handled by the software provider. The organization is responsible for ensuring that the latest signature version is installed on its Information Systems.

Organizational services that are associated with the Intrusion Protection Management service include Security Operations Center (SOC) Monitoring and Incident Management. A SOC is the organization used to monitor, detect and respond to security events, alarms and incidents from information feeds that are passed to it. These feeds may be from Security Information and Event Monitoring (SIEM) applications and other security devices where events may provide insights into malicious activities.

Because performing incident response effectively is a complex undertaking, establishing a successful incident management capability requires substantial planning and resources. Establishing clear procedures for prioritizing the handling of incidents is critical, including implementing effective methods of collecting, analyzing and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal

groups (e.g. human resources, legal) and with external groups (e.g. other incident response teams, law enforcement).

Understanding threats and identifying modern attacks in their early stages is key to preventing subsequent compromises. Proactively sharing Indicators of Compromise (IOC) information among organizations is an increasingly effective way to protect other market participants from cyber attacks.

A more advanced service that is included in this area is cyber threat hunting. This service is the proactive search for intrusions through the identification of Indicators of Compromise and other identifiers that may indicate that the security of the Information System has been compromised.

The Intrusion Protection Management service should be designed to (1) identify malicious activity on Information Systems early in the Kill Chain and (2) activate organizational processes that may eliminate or mitigate cyber attacks to business operations. When combined with Threat Intelligence, this service can become heightened by focusing on specific threats to the organization that may have an increased likelihood to occur.

Involved Roles & Owners
The management of Intrusion Detection tools and applications will require the support of the IT department. In addition, the SOC monitoring may also be conducted by the IT organization or another group that is independent from the management of the Information System.

The organization is responsible for defining its Incident Management process and defining the roles and responsibilities of those individuals/groups that are a part of the process. More advanced organizations in this space may employ cyber threat hunting. When conducting cyber threat hunting, the organization should clearly define those roles, responsibilities and rules of engagement for this testing. Similar to Penetration Testing, this service operates in the production environment and may have adverse effects if not appropriately managed.

Expected Results
Intrusion Protection Management, when implemented and tested periodically, may limit the impact of a cyber attack by providing the organization with the ability to quickly detect and respond to a cyber attack or to identify Information System intrusions early in the Kill Chain. This may limit the probability of business disruption due to cyber attacks. Larger CCPs, CSDs and Custodians should periodically test all aspects of their Intrusion Protection services. While these controls protect individual firms within the Securities Servicing sector, the sector should consider cyber security tabletop exercises to measure the sector's readiness to a material cyber incident. The Intrusion Protection processes will limit the susceptibility of the Securities Servicing sector to cyber attacks and will also serve as a proactive control to protect against certain Market Manipulation risks.

6.7 Security Awareness, Training and Education

Principle & Objective
In order for the internal and external users of Information Systems to consistently apply the desired security precautions to the information and Information Systems, they must receive adequate and effective Security Awareness, Training and Education. In general, Security Awareness is the process used to inform the organization and its users of the desired security behavior. This may be conducted through e-mail, workshops, posters, corporate websites and other communication vehicles. Security Training is used to measure (i.e. test) the effectiveness of Security Awareness communications. This is often

accomplished through scored testing (e.g. security modules, phishing exercises). Security Education is a more specialized security training that is centered on a specific or specialized skill set (e.g. secure coding).

A Security Awareness, Training and Education Program should be focused on the entire organization's population. The content of the Program may be driven by:

- Current and emerging threats
- New regulatory / supervisory rules
- Changes to the organization's perceived threats
- Organizational Key Risk and Performance Indicators data

Depending on the cyber security message, other parts of the risk, compliance, legal and internal audit organizations may be utilized to support the awareness message. The organization should determine:

- The approach it has to communicate awareness messages
- The types of messages (e.g., tag lines, full message format) that are appropriate for that vehicle
- The frequency for which the awareness vehicle may be used

This may be used to develop a Security Awareness, Training, and Education strategy across the organization. In addition to Security Awareness for an organization's employees and contractors, Securities Servicers should also identify the appropriateness of conducting awareness for their third parties and customers and how this communication should be distributed. As cyber attacks begin to target entities that are part of the supply chain for the Securities Servicer sector, these third parties should be made aware of threats that may affect them. This includes activities to ensure the organization's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures and agreements.

Involved Roles & Owners

Security Awareness, Training and Education Programs may be developed within the Information Security or Information Risk organizations. This effort should be supported by other organizational groups which may include Marketing, Communications, Compliance, General Counsel and Audit. The groups may assist in providing message management, content and structure to ensure the correct audience and tone is set for the Program. The responsibility for the development and delivery of Security Training and Education should reside within the Information Security or Information Risk Management groups. Measurement and reporting on the adequacy and effectiveness of this Program would be the role of the second line of defense organization.

Expected Results

Information is one of the organization's most valuable assets, the ability to adequately protect this asset begins with those individuals that develop and / or utilize information and Information Systems to conduct their daily operations; successfully educating these individuals is a key output. This Program provides the users of the organization's information with the knowledge to protect information and the tools needed to safeguard it. A mature Security Awareness, Training and Education Program serves as a mitigating control for all identified Securities Servicers risks identified in Section 3.2 Risk Clusters.

6.8 Independent Reconciliation

Principle & Objective
Reconciliation is a control activity that compares two or more data elements and, if differences are identified, ensures completeness and accuracy. Action is taken to bring the data into agreement if differences are identified (e.g. third party payments vs. services provided, actual vs. projected results, etc.). To be effective, these reconciliation activities should be performed **independently** by different persons or systems, with different input sources and repeatedly across the different stages of a transaction. In this way, any error or fraud at any stage of a transaction can be prevented, detected and corrected at the earliest moment.

Involved Roles & Owners
Involved roles and owners are an organization's business, operational and technical controls staff following the industry and internal control guidelines, with additional lines of defense including internal risk management and audit as well as external counterparty, clearinghouse and regulatory reporting.

Expected Results
Organizations establish and maintain a three (3) lines of defense control environment including independent reconciliation to ensure that any error or fraud at any stage of a transaction can be prevented, detected and corrected at the earliest moment, meeting the risk management goals of their organization, industry and regulators.

6.9 Third Party Risk Management

Principle & Objective
Cyber attacks have extended beyond the direct access of a threat actor to an organization’s information systems. Many third parties have been afforded a certain level of trust and access to an organization’s systems and data. Threat actors have utilized third party connections and services to gain access to an organization’s network. The number of third parties may number in the hundreds for smaller organizations and into the thousands for larger organizations. The proliferation of the use of third parties to conduct business operations has increased the surface area available for these attacks. Many successful cyber attacks (e.g. Target, Panama Papers) have occurred through an organization’s third parties.

An organization must extend the view of its internal threats and risks to those threats and risks posed by the use of its third parties. An organization should maintain an inventory of its third parties, understand the risks that these third parties may have to its business operations and determine what countermeasures, if any, would adequately manage these risks. Due diligence for third parties should take a risk-based approach with greater scrutiny occurring for those third parties that pose the greatest risks to the resiliency of the business operations.

Organizations, where possible, should understand the cyber security risk management posture of their third parties. The Risk Management Lifecycle[5] demonstrates those areas that an organization may review when identifying third party risks and includes:

- Planning
- Due Diligence and Third-party Selection
- Contract Negotiation
- Ongoing Monitoring
- Termination
- Independent Review
- Document and Reporting
- Oversight and Accountability

While organizations and industry groups have taken different approaches to establishing a level of assurance from their third parties (e.g. SWIFT Customer Security Programme, BITS Standard Information Gathering), it should be the decision of each organization how to manage these risks.

Involved Roles & Owners
The management of third party risks begins with the decision of an organizational area to utilize a service. Third party risk extends outside of solely cyber security risks. Third party risks may be operational, financial, contractual and strategic. Therefore, those areas charged with advising the organizational area on these risks should have a process to review these risks and advise the organization of those risks that the service carries. Since risks change over time, the organization should develop a process to review these risks periodically. Given the increased threats from third party relationships, supervisory / regulatory agencies and other standard setting bodies have issued guidance on how these risks should be managed.

Expected Results
Securities Servicers, through the application of a robust third party risk management program, may identify and understand the risks from third party suppliers. Through understanding the risks that clients, counterparties and other market participants pose, organizations can mitigate the loss of significant service offerings and loss of client asset (i.e. asset theft) by working with these entities to build an environment more resilient to those risks.

[5] See OCC Risk Management Guidance at https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html (October 2013)

7. External Framework Elements and Approaches

7.1 Alternative Enforcement Approaches

There are (at least) three alternative approaches to the enforcement of cyber security controls:

- **Voluntary opt in** – 'We will do this because it's the right thing to do'. While this may be impactful in pockets, it is unlikely to affect meaningful change across the market participants. However, this could be reinforced by adoption by a market or industry association.
- **Market / customer pressure** – 'Unless I do this, my customers will decide to go elsewhere'. While this is likely to affect change, it relies on market transparency to allow customers an informed choice.
- **Central enforcement** – 'My overseers are making me do this, otherwise I get fined or lose my license'. This is highly likely to effect change, but relies on action by the third-party supervisor / regulator to demonstrate negligence to a certain threshold.

7.2 Implementation of a Risk-Based Approach

Regardless of whether risk mitigation is enforced by regulation or set by client or industry expectations, the cornerstone of a risk mitigation program is the implementation of a holistic comprehensive cyber strategy that should be mandatory for globally and domestically systemically important entities.

This risk-based approach should measure and prioritize the threats to the organization. This approach could include the consideration of forward-looking threat intelligence, system vulnerabilities and potential business operational impacts.

7.3 Three Lines of Defense Risk Management Strategy

The Three Lines Of Defense controls for effective risk management was put forth by the Institute of Internal Auditors (IIA) as a means for organizations to develop clear responsibilities within their risk and control structure. The three lines of defense include:

- Management Control (First Line)
- Risk Control (which may include Security teams) and Compliance (Second Line)
- Independent Assurance, such as Internal and External Audit (Third Line)

Governing bodies and senior management are not considered as part of the three lines but are the primary stakeholders for which the lines serve.

The business management owns and manages risk and forms the first line of defense. It is responsible for implementing risk mitigation strategies to manage control deficiencies. Business Management is also responsible for the day-to-day management of internal controls. This group may define detailed procedures that outline how these controls may be implemented.

The second line of defense is established by the different risk management and compliance functions. These functions assist the building and monitoring of the first line of defense controls. The second line of defense may intervene in modifying and developing internal

controls (e.g. through providing business advisory on risk management implementation). Given this role, the second line of defense cannot offer true independent analyses to governing bodies and senior management and internal controls. Key functions for the second line of defense includes:

- Governance through the selection of control frameworks and the definition of policies and standards
- Measuring the adherence to the defined policies, standards, supervisory rules and guidance from standards setting bodies
- Identifying current and emerging threats
- Reporting on the effectiveness of controls, compliance with laws and regulation and the remediation of deficiencies

The third line of defense is established through the internal audit organization. Internal audit provides assurance on the effectiveness and manner with which the first and second lines conduct their risk management activities. Additionally, internal audit should provide an independent opinion of the adequacy and effectiveness of the organization's risk control activities.

7.4 Recovery from a Cyber Attack

In many instances, institutions take a similar business continuity approach to cyber attacks as they do for physical attacks. However, cyber attacks fundamentally differ from physical attacks, rendering many traditional business continuity mechanisms ineffective in protecting against cyber attacks. The following is provided from DTCC and Oliver Wyman, 'Large-scale Cyber-Attacks on the Financial System', March 2018.

Detection: A physical attack occurs as a result of an external, visible event, while a cyberattack may happen imperceptibly, or as a result of a new attack type that may not be immediately known. In addition, cyber attackers often employ methods to cover their tracks.

Response: The impact of a physical attack is usually realised immediately after the attack, is contained and is easy to pinpoint. On the contrary, cyber attacks have the potential to quickly spread and the full extent of the impact is not immediately clear.

Recovery: Recovery from physical attacks optimizes for immediate resumption using alternate processes and back-up applications or geographically dispersed data centers. Recovery from a cyber attack needs to balance speed of resumption with potential negative consequences resulting from premature resumption (for example, proliferation of malware to additional internal systems or external partners).

Consequently, response and recovery from a cyber attack can be a lot more challenging compared to a physical attack. The detection and effective analysis of a cyber attack can be considerably more time-consuming as analysts grapple with potentially unknown threat vectors, impacting the ability to quickly and effectively mitigate, resume and remediate. For example, if attackers manipulate data imperceptibly over a period of time, successfully bypassing reconciliation controls, pinpointing when the corruption started and reverting to a last known good state can be challenging.

Contagion can make a cyber attack challenging to contain and complicate the decision of resumption. For example, if data gets corrupted at a major data feed provider, the corruption may potentially propagate to a number of downstream data users, particularly smaller institutions that leverage only one major data provider. In addition, the lack of tailored requirements and expectations for specific cyber scenarios and limited

industrywide testing may impact the ability of the financial services industry to react fast during a cyber attack. This is compounded by insufficient clarity around leadership in the case of key decisions, such as calling an 'all clear' and determining when affected firms may resume operations. Lastly, critical financial services activities tend to be concentrated in a few highly regulated entities, which means a cyber attack on any one of them can cripple entire sub-sectors and markets. The sophistication and complexity of cyber attacks is growing, rendering traditional back-up mechanisms and redundancies ineffective. For example, a sophisticated cyber attack which strategically affects production data as well as data backups at multiple institutions would significantly complicate the restoration of critical data.

ISSA believes that while Securities Services firms must have their own Recovery Playbooks to ensure a coordinated approach within the securities servicing industry, two potential cross-industry coordination initiatives may be beneficial:

7.4.1 Collective Response and Recovery Plan, Outlining Key Response and Recovery Requirements

This initiative calls for collaborating on an outline of collective actions to be taken upon detection of a large-scale cyber attack, based on a set of standardized criteria and tailored to specific cyber attack scenarios.

The securities servicing industry currently lacks alignment and clearly defined standards pertaining to critical response and recovery considerations, including:

1. Definition of resumption and recovery
2. Criteria for safe resumption of operations
3. Agreement on appropriate timeframes for resumption and recovery
4. Plans for communicating with the public during a large-scale cyber attack

7.4.2. Contingent Service Arrangements

This initiative includes arrangements that allow securities servicers to continue critical operations in the event that they or a partner suffer an outage from a cyber attack. Given the complexity and broad scope of potential impacts of large-scale cyber attacks, such as the outage of key players or compromise of backups, no single entity has all required capabilities and capacities to address all possible attack vectors and shore up all possible vulnerabilities. Regardless of the level of preparedness, there may be situations where a key payment, clearing and settlement provider is unable to fulfil its services for an extended period of time, creating the need to resort to contingent service arrangements.

The ISSA Working Group on Cyber Risk will track industry initiatives in these two areas and look to participate to bring in the perspective of securities servicers.

7.5 Practical Points for Senior Management

Senior Management responsible for their organization's cyber risk mitigation overarching framework and detailed plan should consider the following points in satisfying their obligations in the protection of their firm. They should:

- Ensure that dedicated, segregated, experienced and capable **cyber security teams** led by a role akin to a Chief Information Security Officer exist and are properly funded. These teams are responsible for monitoring threat levels through an appropriate threat intelligence network, monitoring industry standard cyber security frameworks and continuously benchmarking these against those deployed by the

firm. These teams ensure that risk / threat driven priorities are established with appropriate financial and enterprise-wide support from the managing bodies.

- Understand the core components and principles of the **cyber security framework** as it pertains to their jurisdiction as well as the principles of global standards.
- Ensure that a core part of the deployment of the framework includes repeated, frequent **staff awareness** of the cyber threats and the practices they must follow, particularly countering the phishing threat with testing regularly conducted.
- Ensure the cyber framework plan is prioritized for **Board-level attention** and sufficiently funded with necessary FTE and CapEx investments to allow implementation of the necessary cyber security controls.
- Ensure timely **management reporting** with regular assessment, risk tracking and progress reporting to senior management.
- Understand that firm-wide cyber security programs are operating effectively within the firm with **independent assurance** / audit to validate this.
- Understand the criticality of services provided by **vendors** and the impact that a cyber attack on them can mean and that vendor cyber security programs and policies are acceptable to the firm including the right to audit critical service vendors.
- Have a clear **response / crisis management playbook** that includes a rapid impact assessment including identifying the point at which systems should be shut down. This includes who has the authority to give this order together with a considered and timely communication plan to all stakeholders, including clients, counterparties, regulators, staff, vendors and industry groups including threat intelligence agencies
- Have **alternate procedures** documented at the 'how' level, setting out roles and responsibilities, key contacts, sequence of task performance and required timings for completion of these tasks. Regularly perform cyber attack simulation tests prioritized by critical services, involving key business, IT and operations management with oversight from expert cyber security and risk management personnel.

Provision of these measures and the detailed controls allows cyber risks to become manageable, but not eliminated, as they are treated just like any other risk within the enterprise.

8. Appendices

Appendix 1 - Use Case 'SWIFT Customer Security Programme'

In 2016, SWIFT launched the Customer Security Programme (CSP) in response to the attack on Bank of Bangladesh. CSP supports all customer segments in reinforcing the security of their local SWIFT-related infrastructure. The program is structured around three components and applies to all SWIFT customers:

1. **You - Secure and Protect.** Further enhancement of SWIFT tools and interfaces, plus the adoption by the community of formal Security Controls – attestation, compliance, counterparty consultation, all using the KYC-SA tool
2. **Your Counterparts - Prevent and Detect.** Transaction Pattern Detection, RMA, DVR and 'In Flight' Sender Payment Controls
3. **Your Community - Share and Prepare.** Intelligence Sharing and SWIFT ISAC

Profile of Advanced APT Attacks in Institutional Payments

Threat Actor Motivation Profile

- Financial gain

Threat Actor Profile

- Organized crime and / or nation states
- Well funded, highly motivated
- Sophisticated and patient
- Coordinated

Attack Vector Profile

- Highly targeted APT attacks with custom malware seeking high-yield targets and valid operator / approver login credentials
- Very long reconnaissance period, e.g. 200 days giving deep understanding of business flows and operational processes
- Attacks over public holidays and same-day attacks across multiple victims
- Initial entry via e-mail phishing, rogue web sites, USB stick and / or insiders

Victim Profile

- Small, regional banks that use the SWIFT network
- Payments instruments only
- Cross-border transactions
- Use correspondent banking chain

CSP Programme Key Takeaways

- CSP took an agnostic approach, it covered all markets and all instrument types, for all SWIFT customers.
- CSP reuses existing security frameworks and standards, e.g. ISO 27002, NIST and PCI-DSS, to define the mandatory and advisory controls.
- CSP reports customers' level of compliance to local regulators.
- CSP enables transparency - each customer attests their compliance, which is made available to their counterparties. Each counterparty then manages their level of business risk accordingly.
- CSP promotes the sharing of cyber information with intelligence agencies.
- CSP undertook active, extensive and prolonged engagement with the community.

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'.
Cyber Event	An observable 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 for its intended users
Indicators of Compromise	A piece(s) of forensic data that identifies potential malicious activity on an Information System
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 organization is exposed
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-mail to request information from users or direct them to fake websites that request information

Term	Definition
Ransomware	A type of malicious software that prevents or limits users from accessing their system either by locking the system screen or files until a ransom is paid
Spearphishing	A digital form of social engineering that uses an authentic-looking - but bogus - e-mail to request information from a distinctive set users (e.g. corporate executives) in an attempt to have them provide sensitive information
Tactics, Techniques and Procedures (TTP)	The behavior of a threat actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures are an even lower-level, highly detailed description in the context of a technique
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 Defense	A management risk control framework which consists of three levels used to provide oversight of an organization’s risks
Unauthenticated Vulnerability Scanning	A scan that attempts to discover vulnerabilities on an Information System through limited system access
Waterholing 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 - Working Group Members

Working Group Member	Organisation
Andy Smith (Lead)	BNY Mellon
Thomas Koch (Sub Lead)	SIX Group
Brett Lancaster (Sub Lead)	SWIFT
Roger Harrold	AlfaSec Advisors
Terry Ferrao	Citibank
Bhavesh Jani	Citibank
Irene Mermigidis	Clearstream
Nejib Zaouali	Clearstream
Bruce Butterill	DCV Chile
Emma Johnson	Deutsche Bank
Bill Hodash	DTCC
Jason Harrell	DTCC
Tony Freeman	DTCC
Pavel Lozhkin	NSD Russia
Manoj Sarangi	NSDL India
Josef Landolt	ISSA
Goran Fors	SEB
Nino Ciganovic	SIX Group
Jyi-Chen Cheuh	Standard Chartered
Samantha Finan	Standard Chartered

In addition to the core Working Group members, the initial hypothesis of cyber security risks was tested and validated by ~30 experts who actively participated in the breakout working sessions at the ISSA Symposium in May 2018.