DTCC

Securing Today. Shaping Tomorrow.®

OLIVER WYMAN

MARCH 2018

LARGE-SCALE CYBER-ATTACKS ON THE FINANCIAL SYSTEM

A CASE FOR BETTER COORDINATED RESPONSE AND RECOVERY STRATEGIES

FOREWORD

Large-scale cyber-attacks on critical financial infrastructure are a major threat, potentially causing significant damage and disruption to the financial sector and the larger economy. The complexity of the financial services industry, the interconnectedness of individual players, and the introduction of new and innovative technologies further heighten the risk of a large-scale cyber-attack on the financial sector. Systems breakdowns are inevitable because the modern financial system is open and, therefore, more susceptible to attack. Both the public and private sectors must mobilize themselves to be well prepared.

We need to focus on building resilience. In contrast, most efforts to date have focused on putting in place mechanisms to reduce the likelihood of a successful large-scale cyber-attack. Realistically though, it is a question of when, not if, a large-scale attack succeeds. This reality, combined with the increased complexity and diversity of cyber threats, requires firms to be prepared to detect problems and recover from them as efficiently as possible. The Depository Trust & Clearing Corporation (DTCC) and Oliver Wyman believe that effective response and recovery requires continued industry collaboration and, in some cases, common industry utilities and approaches, in support of the efforts currently underway. In this paper, we describe how this could be done.

We would like to thank the more than 50 subject matter experts, and numerous industry working group participants, who supported the fact finding, hypothesis generation, and derivation of solutions during the development of this white paper. We look forward to engaging with our industry colleagues on these issues and advancing this important dialogue with concrete steps to increase resilience.

Andrew Gray
Group Chief Risk Officer at DTCC

Paul Mee
Partner at Oliver Wyman

TABLE OF CONTENTS

Executive summary	3
Large-scale cyber-attacks	4
Response and recovery challenges	7
Opportunities for more industry coordination	9
Moving forward	15
Appendix A. Opportunity descriptions	16
Appendix B. Response and recovery lifecycle	21
Appendix C. Bibliography	22
Appendix D. Acknowledgments	23

EXECUTIVE SUMMARY

Cyber-attacks on financial institutions are becoming more frequent, complex, and sophisticated, with potential for far-reaching, systemic impacts. The motivation of cyber-attackers is shifting from purely achieving financial gains to disrupting critical infrastructures, such as through nation-state attacks, which threatens the basis for confidence in the financial system and even national or international stability.

In today's world of geopolitical turmoil and the ever-increasing speed of technological innovation, the threat from actors with the necessary motivation, financial means, and technological capabilities, is real. Hence, the orchestration of a large-scale cyber-attack is likely a matter of "when", not "if".

This report represents the outcome of a joint effort of DTCC and Oliver Wyman to bring together financial services and non-financial services practitioners to investigate cross-industry coordination on response and recovery mechanisms to mitigate the systemic consequences of a large-scale cyber-attack. We based our findings and recommended initiatives on extensive research, interviews with more than 50 subject matter experts, and advice from an industry working group[1] comprising key cybersecurity and business continuity practitioners (Appendix D).

As a result of this effort, two potential cross-industry coordination initiatives were prioritized for further consideration.

- **COLLECTIVE RESPONSE & RECOVERY PLAN, OUTLINING KEY RESPONSE AND RECOVERY REQUIREMENTS:** Tangible 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.
- **CONTINGENT SERVICE ARRANGEMENTS:** This initiative includes arrangements that allow financial institutions to continue critical operations in the event that they or a partner suffer an outage from a cyber-attack.

The mechanisms and approaches designed through these initiatives are meant to supplement initiatives currently in place or under development by industry coordination groups (for example in the U.S., Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Financial Systemic Analysis and Resilience Center (FSARC)[2]). Refinement, detailing and implementation of the proposed initiatives will require continued mobilization of the industry as well as relevant public sector bodies. This paper focuses on the implementation of potential initiatives for the U.S. financial system. But, in general, the coordination opportunities identified in this paper apply similarly to financial markets in other jurisdictions and should be considered by local regulators and industry coordination groups.

In the remainder of this document we investigate three areas to make the case for stronger industry coordination during response and recovery in the event of a large-scale cyber-attack.

- **LARGE-SCALE CYBER-ATTACKS:** Key attack types and scenarios for large-scale cyber-attacks with systemic consequences in the context of the payment, clearing, and settlement ecosystem.
- **RESPONSE AND RECOVERY:** Challenges faced by the industry to respond and recover fast and effectively from a large-scale cyber-attack.
- **OPPORTUNITIES FOR MORE INDUSTRY COORDINATION:** Set of initiatives to strengthen industry-wide coordination and increase effectiveness response and recovery strategies.

[1] Working group consisted of members from a subset of the institutions mentioned in Appendix D Acknowledgments

[2] See Box 1 for more detail

LARGE-SCALE CYBER-ATTACKS

Payments, clearing, and settlement services are critical to the financial services industry and essential for the smooth functioning of the global financial system and the economy overall. Wholesale payments services enable financial institutions and corporations to send payments domestically and across borders. Securities clearing and settlement services include central custody of securities and facilitate the exchange of securities on behalf of buyers and sellers. A disruption of these services can significantly impact the functioning of financial markets by, among other things, impeding credit and liquidity flows.

In the context of an increasingly interconnected financial ecosystem[3], an attack on one or more institutions or critical infrastructures can have significant ripple effects that "cascade into related ecosystem components (for example a bank transacting with the financial infrastructure or its customers), resulting in significant adverse effects to public health or safety, economic security or national security."[4] In other words, even an isolated cyber-attack on one or more payments, clearing and/or settlement firms could quickly become large-scale and have systemic consequences.

In today's complex geopolitical climate, the potential for large-scale cyber-attacks continues to exist. Groups backed by nation-states with politically motivated agendas represent the biggest risk, given that they have both the motivation and necessary resources to orchestrate large, complex cyber-attacks.

These types of attacks represent a significant risk for payments, clearing and/or settlement firms, given the criticality of their operations and the interconnectedness of their activities. Payments, clearing and/or settlement firms are actively investing in cyber defenses, and the importance of industry-wide cooperation is a subject high on the agendas of many of these firms, as evidenced by their engagement in the activities of industry coordinating bodies. For example, in the U.S., many firms are engaging on this topic through two available financial services industry coordination forums: FS-ISAC and FSARC *(See Box 1 for more detail)*.

BOX 1: FS-ISAC AND FSARC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was founded in 1999 and serves as the primary cyber and physical threat information sharing organization around the globe. As its membership has grown to nearly 7,000 institutions, the FS-ISAC has expanded its capabilities to include threat analysis, incident response planning, exercises, the sharing of best practices, and educational events.

The Financial Systemic Analysis and Resilience Center (FSARC) was formed in 2016, under the FS-ISAC, to expand the sector's ability to mitigate systemic risk to the U.S. financial system from cyber threats. Its primary roles include intelligence sharing, analysis of threats, vulnerabilities, and trends, analysis of systemic threats, and cybercrime coordination.

[3] The payments, clearing, and settlement ecosystem includes buyers, sellers, custodian banks, clearing and/or settlement institutions, exchanges, and broker-dealers

[4] World Economic Forum, "Understanding Systemic Cyber Risk," 2016

In general, cyber-attacks can be characterized by type and impact *(Figure 1)*. Any of these attack types can be highly disruptive in nature. But in our interviews and working group discussions with industry experts manipulation of critical data was raised as the attack type that is most likely to have systemic consequences for three main reasons:

- **DETECTION:** Difficulty to identify that an attack has occurred, particularly if data manipulation is executed without detection, bypassing reconciliation controls. For example, FireEye [5] found that it takes on average 146 days for firms to detect a cyber intrusion.[6]

- **RESPONSE:** Difficulty to establish when and how the attack originated, especially in an interconnected system with multiple options for breach origination, and resulting inability to respond quickly.

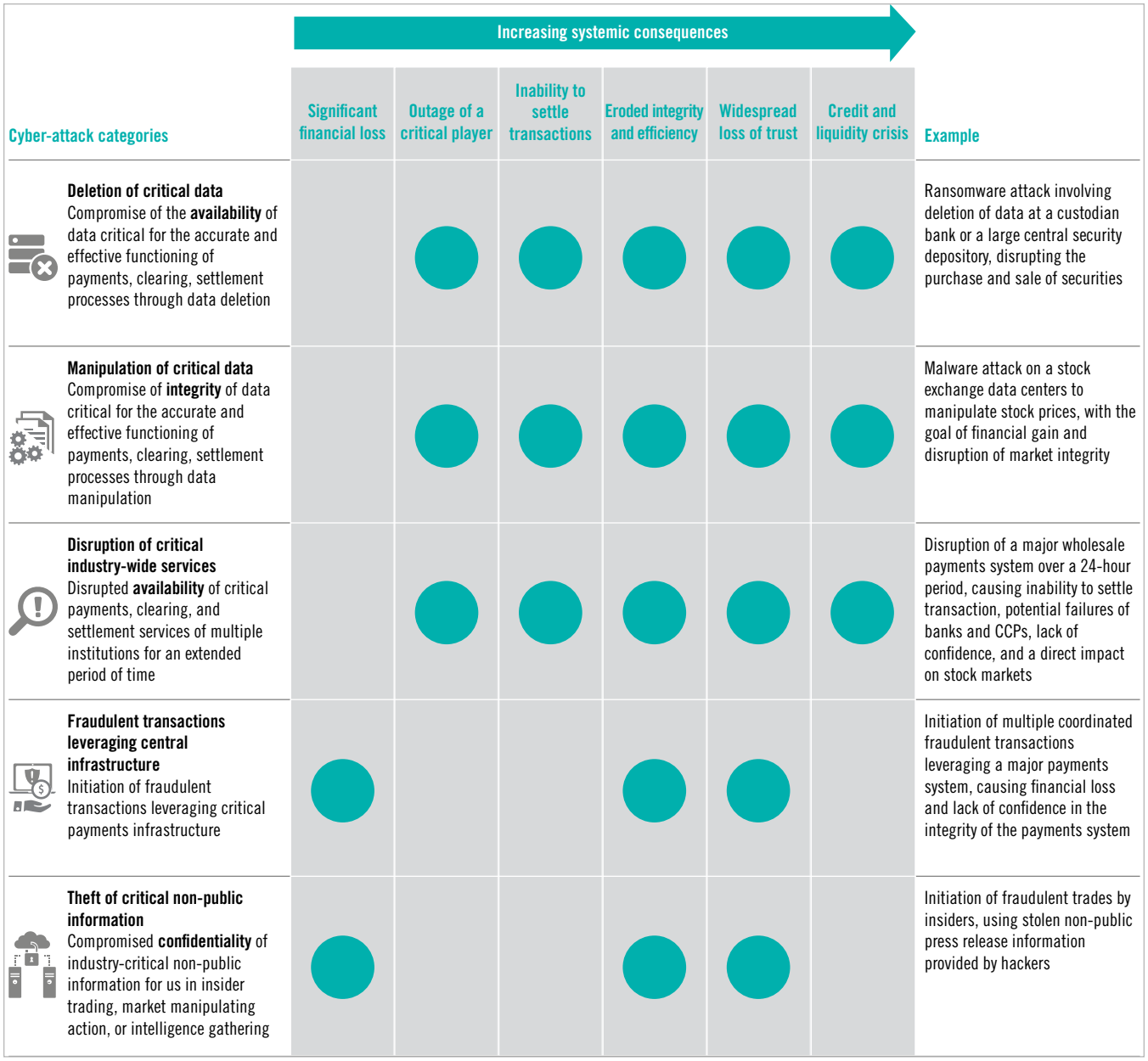
- **RECOVERY:** Difficulty to identify and revert back to the 'last known good' state of data, given that analyzing and diagnosing data manipulation can be complicated and time consuming.

If the corruption of data integrity is particularly pervasive and harmful, it could result in the disabling of key market players, causing financial loss, disruption of critical financial services activities, and cascading effects throughout the economy.

[5] FireEye, Inc. is a publicly listed enterprise cybersecurity company that provides products and services to protect against advanced cyber threats, such as advanced persistent threats and spear phishing.

[6] FireEye and Marsh & McLennan, "Cyber Threats: A perfect storm about to hit Europe?", 2017

Figure 1: Cyber-attack types and impacts



Given the potential for significant cascading and contagion effects, payments, clearing and/or settlement firms have built-in redundancies to ensure the potential impact of the failure of any single systemically important institution on the system can be mitigated. For example, established reconciliation processes ensure that positions held at central securities depositories (CSDs) match those held at custodians and member banks. However, the redundancy mechanisms built into individual firms may not be as effective in the event of smaller distributed attacks that impact multiple firms simultaneously.

While developing an exhaustive list of potential cyber-attack scenarios is not feasible, the industry needs to continue identifying potential patterns of attack that have the potential for creating systemic impacts as a key input into the design and implementation of industry-wide response and recovery mechanisms.

RESPONSE AND RECOVERY CHALLENGES

In many instances institutions still take a traditional business continuity approach to physical attacks to preparing for cyber-attacks. However, cyber-attacks fundamentally differ from physical attacks, rendering many traditional business continuity mechanisms ineffective in the cyber context.

- **DETECTION:** A physical attack occurs as a result of an external, visible event, while a cyber-attack 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 realized 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 diverse 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 *(Figure 2)*.

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 industry-wide 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.

Figure 2: Challenges to response and recovery

Uncertainty around the origin, time and point of impact of a cyber-attack, and challenges around data sharing and fast collection of relevant information from a large number of partners complicates diagnostics

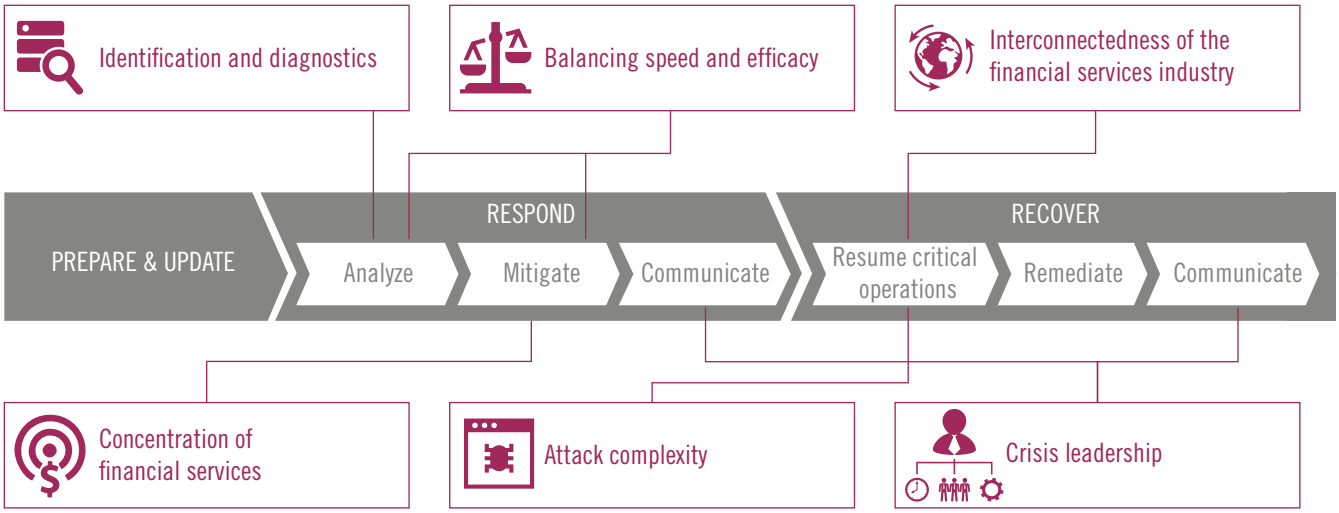
Data manipulation is executed imperceptibly, bypassing reconciliation controls, complicating the ability to pinpoint when the corruption started and revert to a last known good state

Lack of tailored requirements and expectations for specific cyber-scenarios and lack of fully effective industry-wide testing may challenge fast industry-wide recovery

No alignment on a practical and safe definition of resumption leads a stricken firm to resume operations prematurely

Connectivity of the financial system facilitates the spreading of a cyber-attack across financial infrastructures, financial institutions and geographies

The corruption of data integrity at a major data feed provider (e.g., Bloomberg, Reuters) propagates throughout the financial system



The concentration of critical financial services activities in a few highly regulated entities and the increasing usage of cloud providers could exacerbate the consequences of a successful large-scale cyber-attack

The debilitation of a major clearing and settlement institution leads to collapse in the price of a certain product, typically cleared through that institution

Defining adequate response and recovery strategies is difficult given the broad scope of potential impacts of cyber-attacks (e.g. compromise of backups, coordinated attacks on multiple sectors)

A sophisticated cyber-attack affects production data as well as data backups at a given institution, complicating the restoration of critical data

Insufficient clarity around leadership may hinder key decision-making (e.g. affected firms re-joining the network, appropriate message to the media, giving an "all clear") and coordinated communication to the public

Firms which have disconnected a given stricken counterparty are uncertain as to when to safely allow reconnection

OPPORTUNITIES FOR MORE INDUSTRY COORDINATION

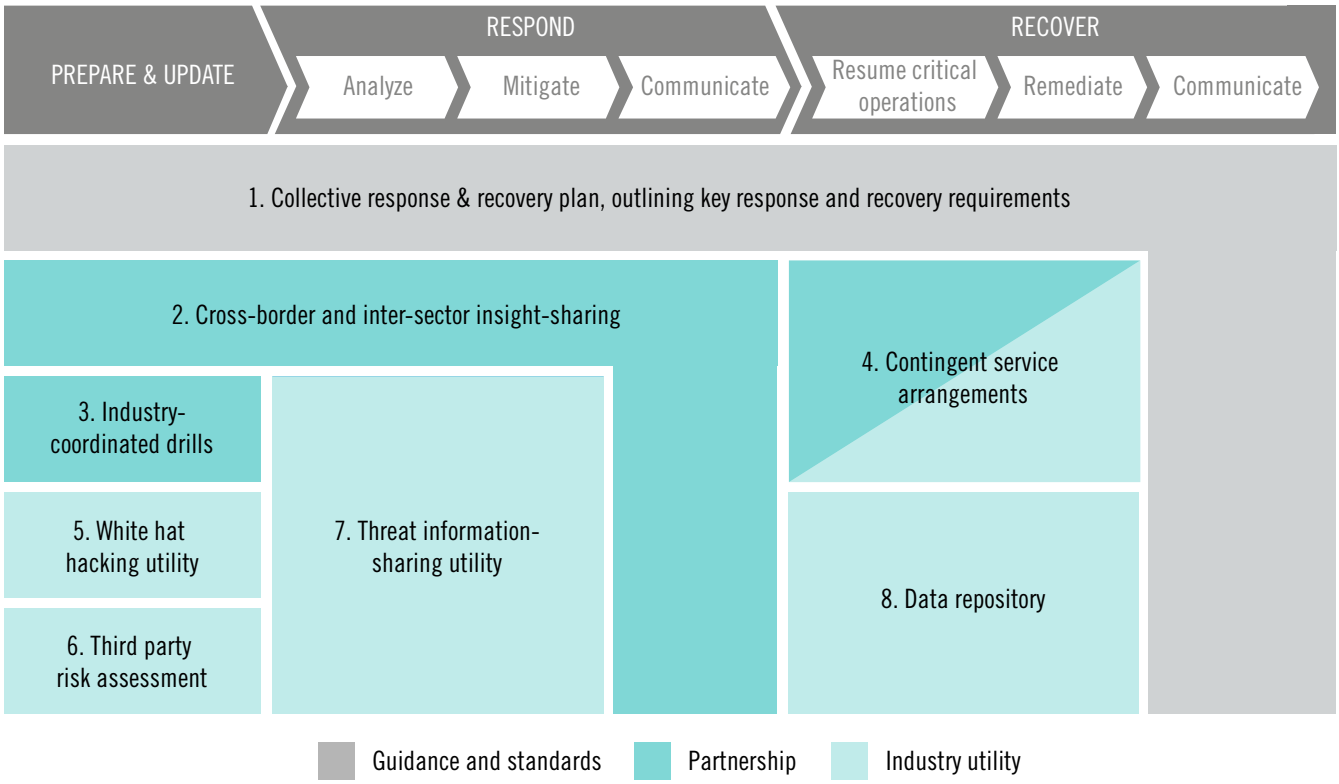
Addressing these challenges will require even stronger coordination among payment, clearing and/or settlement firms on response and recovery approaches going forward.

In the past, firms have placed much focus on preventative cybersecurity measures. Recently, mechanisms to support and facilitate effective response and recovery are gaining momentum (for example, FSARC, Sheltered Harbor initiative[7]). But the regulatory landscape remains fragmented with limited guidance around response and recovery beyond basic principles. Therefore, it is imperative for the industry to proactively develop and agree on response and recovery standards that will facilitate effective response and recovery, and adherence to high-level regulatory principles.

With this objective in mind, we, in cooperation with a panel of industry experts, developed a set of recommendations to supplement and further strengthen existing industry-wide coordination efforts across the response and recovery lifecycle and across a variety of implementation mechanisms *(Figure 3)*.

In defining these opportunities, we considered implementation through guidance and standards, which provide the foundation for consistency of response and recovery strategies at individual firms, as well as implementation through explicit partnerships or industry-maintained utilities, which enable closer cooperation and efficiency of resource investment.

Figure 3: Potential opportunities for stronger industry coordination across the response and recovery lifecycle



[7] Sheltered Harbor is a voluntary industry initiative for secure storage and rapid reconstitution of retail bank customer account data. Data is stored in a distributed fashion in a Sheltered Harbor specified data vault, it is kept private by each institution and is encrypted.

We prioritized these opportunities based on impact and feasibility.

1. **IMPACT:** Combination of **(a)** capacity to reduce the severity of a successful large-scale attack **(b)** ability to improve speed and effectiveness, and **(c)** degree of distinctiveness from existing initiatives
2. **FEASIBILITY:** Combination of **(a)** design complexity, **(b)** likelihood of adoption, and **(c)** degree to which the initiative's financial or business cost is outweighed by its expected benefits

This prioritization surfaced two major initiatives for strengthened industry cooperation on response and recovery:

1. **Collective response & recovery plan, outlining key response and recovery requirements**
2. **Contingent service arrangements**

OPPORTUNITY 1: COLLECTIVE RESPONSE & RECOVERY PLAN, OUTLINING KEY RESPONSE AND RECOVERY REQUIREMENTS

CHALLENGE ADDRESSED

The financial services 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**

While regulators have published a set of high-level guidance (for instance, the CPMI-IOSCO international guidelines on cyber resilience for financial market infrastructures), concrete standards mostly do not exist today.

The lack of alignment on standards creates challenges in addressing existing regulatory expectations (for example, requirements around the 2-hour recovery objective), which may preclude the financial services system as a whole from reacting effectively during a large-scale cyber-attack. In this scenario, institutions may be unable to make resumption decisions in a consistent manner, based on criticality of operations affected and risk associated with resumption of operations.

Insufficient clarity around communication plans, particularly to clients, investors and the broader public, during a large-scale cyber-attack could prevent the industry from effectively avoiding widespread loss of confidence and the potential deepening of an economic crisis.

PROPOSED INITIATIVE

The proposed initiative entails developing a tangible 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 concepts build on the existing FS-ISAC All Hazards Crisis Response Coordination playbook which provides guidance to the financial sector on how to evaluate and respond to physical or cyber crises, share information and

analysis, and coordinate with government and other partners. In addition, it supplements the response and recovery playbooks FSARC is currently developing for specific systemic cyber-risk scenarios.

The proposed initiative supplements these capabilities by stipulating the development of concrete response and recovery standards, tailored to specific cyber-attack scenarios, and further empowering existing governance bodies to offer recommendations on resumption decisions critical for the entire system. To ensure this critical component is utilized effectively, standards and criteria should be incorporated into the FSARC response and recovery playbooks.

DESIGN ELEMENTS

- Identification of key response and recovery considerations requiring alignment
- Clear definition of standards, tailored to specific cyber-attack types and codified into actionable playbooks
- Establishment of a mechanism for demonstrating compliance with defined standards and performing independent validation
- Creation of a governance body (or expansion of the mandate of an existing one, such as the FS-ISAC CERG) to assess and challenge the evidence provided, offer a non-binding recommendation, and serve as an overall advisory board

KEY BENEFITS

- **IMPROVED RESILIENCE** of the overall financial system by ensuring firms are held up to a minimum set of acceptable standards and minimizing the threat of contagion
- **EFFECTIVE, SPEEDY COLLECTIVE ACTION** during a systemic cyber-attack that prioritizes the common good
- **INCREASED CUSTOMER AND INVESTOR** confidence, driven by the knowledge that the industry is following a set of commonly agreed upon standards
- **INCREASED TRANSPARENCY** and confidence among institutions

BOX 2: EXISTING RESPONSE AND RECOVERY PLAYBOOKS AND GOVERNANCE

In the event of an industry-wide cyber attack, the financial services sector can follow the broad guidance in the All Hazards Crisis Response Coordination playbook maintained by the FS-ISAC. The playbook describes the key governance and escalation bodies to be activated in the aftermath of a cyber-attack, including:

- **THREAT INTELLIGENCE COMMITTEE (TIC):** Facilitates the dissemination of information, analyzes incident, and facilitates impact assessment and crisis escalation to the Core Executive Response Group (CERG). Includes FS-ISAC members.
- **BUSINESS RESILIENCY COMMITTEE (BRC):** Provides systemic incident response guidance, analyzes incident, and facilitates impact assessment and crisis escalation to the CERG. Includes FS-ISAC members.
- **MEDIA RESPONSE TEAM (MRT):** Validates facts and coordinates messaging on behalf of the financial services sector. Includes FS-ISAC members and may include members from FSARC and industry associations depending on the event/crisis.
- **CORE EXECUTIVE RESPONSE GROUP (CERG):** Gathers subject matter experts to determine event impact and determine if Crisis Management Team activation is needed, whose role is to facilitate partner collaboration and member communication. Includes key sector representatives, executive leadership of the Financial Services Sector Coordinating Council (FSSCC), FS-ISAC, SIFMA, FSARC, Sheltered Harbor and TIC, BRC, MRT Chair(s), and U.S. Treasury, and others as needed.

These sector-level capabilities are further supplemented by U.S. government resources available in the event of a cyber-attack with national security implications. In such an event, the Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force, is the lead agency for threat response activities, including investigative, forensic, analytical, and mitigation activities.

OPPORTUNITY 2: CONTINGENT SERVICE ARRANGEMENTS

CHALLENGE ADDRESSED

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 fulfill its services for an extended period of time, creating the need to resort to contingent service arrangements.

PROPOSED INITIATIVE

This initiative includes arrangements that allow financial institutions to continue critical operations in the event that they or a partner suffer an outage from a cyber-attack, through one of the following operating models:

1. **Individual firm backup infrastructure to perform critical functions**
2. **Arrangements between private institutions to provide mutual assistance in support of critical payments, clearing, and settlement activities**
3. **Industry utility designed to perform critical operations of several financial institutions (for example, through a request for technical assistance)**

The FSARC has already advanced the thinking on this topic through the Wholesale Payments Initiative (WPI) playbook. The playbook recommends that financial institutions set up back-up accounts with a peer firm for their largest / most critical accounts, allowing for continued servicing of these accounts in case of an outage.

In addition, the Sheltered Harbor initiative, spearheaded by the FS-ISAC, requires banks to proactively store retail customer account data in an industry-standard format, allowing for a peer bank to restore account information and keep a stricken business up and running *(See Box 3)*.

BOX 3: SHELTERED HARBOR INITIATIVE

Sheltered Harbor is a voluntary industry initiative undertaken by the U.S. financial services sector to enhance the sector's resiliency, and to provide additional protections for consumer account information. Its goal is to extend the industry's capabilities to securely save and restore account data in the event of a loss of operational capability.

This solution is implemented via the Sheltered Harbor Specification, which covers the operational and technical requirements for protecting consumer account data. Participating financial institutions extract critical account data, convert it to an industry standard format, validate, encrypt, and transmit to a Sheltered Harbor vault on a continous basis. Upon Sheltered Harbor activation, an affected participant retrieves and transmits its data to a Restoring Institution, which decrypts and restores core data.

Consumer data stored in a Sheltered Harbor data vault is kept private by each institution, encrypted and protected from change. The Sheltered Harbor model assumes no central repository for protected accounts.

Implementing arrangements in line with the principles outlined in the WPI playbook is a key step in the direction of ensuring greater stability in the financial system. Next, the industry needs to identify additional use cases where contingent arrangements would be beneficial and evaluate the benefits and feasibility of establishing industry-owned utilities.

DESIGN ELEMENTS

- Alignment on which financial services activities are critical from a systemic lens and require protection through contingent service arrangements
- Further investigation to identify the most appropriate operating model and scope out the solution
- Clear articulation of timeframe within which alternate arrangements are expected
- In the case of a partnership or utility model, standardization of data formats and taxonomies
- In the case of individual firm contingent arrangements, support from regulators to drive adoption

KEY BENEFITS

- **INCREASED RELIABILITY OF CRITICAL FINANCIAL SERVICES** operations and reduced instability and economic gridlock during a large-scale cyber-attack
- **REDUCED POTENTIAL FOR CONTAGION** by limiting likelihood of a critical player rejoining the financial system prematurely, due to the absence of a substitute service provider
- **INCREASED CUSTOMER AND INVESTOR CONFIDENCE,** driven by the availability multiple layers of protection to facilitate continuity of critical industry activities

MOVING FORWARD

Preparing effectively for a severe but plausible large-scale cyber-attack requires working together to make difficult decisions for the greater good. Organizations such as FS-ISAC and FSARC have taken important steps in the right direction and are well positioned to help drive some of the opportunities described in this paper forward.

While this study surfaced the two proposed initiatives as recommended for prioritization by the industry, further discussion of the remaining options for coordination outlined in the Appendix should remain on the agendas for industry-wide forums.

Refinement, detailing and implementation of the proposed initiatives will require a five-step approach:

1. **Assignment of ownership and responsibilities for the initiatives,** including assignment of primary owners and identification of additional key stakeholders and their responsibilities.
2. **Mobilization of the appropriate industry stakeholders,** including financial services and non-financial services representatives practically responsible for design and deployment of capabilities required at each stage of the response and recovery lifecycle.
3. **Detailing of each initiative,** including scope, ownership structure, execution model, and enforcement mechanism.
4. **Development of a structured implementation plan,** considering achievable timelines, resource commitment, and industry buy-in.
5. **Phased implementation** that considers which industry players need to be integrated into the solution and prepared most rapidly, and incorporates effective testing approaches beyond tabletop exercises.

The mobilization of a broad set of experts and stakeholders will be particularly critical for the second proposed initiative, given the associated scope and design complexity, as well as the significant time required for its operationalization.

In addition, the public sector needs to play a role when legislative support is necessary to implement industry-wide and cross-border efforts, both in terms of providing incentives and helping resolve roadblocks related to misaligned legislative frameworks.

Ultimately, the industry cannot rely on the low feasibility of cyber-attacks with systemic consequences. Rapid mobilization and commitment is required to ensure safety and soundness of the financial industry.

APPENDIX A. OPPORTUNITY DESCRIPTIONS

I. GUIDANCE & STANDARDS

1. COLLECTIVE RESPONSE & RECOVERY PLAN, OUTLINING KEY RESPONSE AND RECOVERY REQUIREMENTS

Challenge:

Lack of tailored requirements and defined standards for specific cyber-scenarios may impact the ability of the financial services system as a whole to react effectively during a large-scale cyber-attack with systemic consequences.

Opportunity:

Outline of collective actions to be taken upon detection of a large-scale cyber-breach with systemic consequences, based on a set of standardized criteria, tailored to specific cyber-attack scenarios.

Impact:

1. Improved resilience of the overall financial system by ensuring firms are held up to a minimum set of acceptable standards and minimizing the threat of contagion.
2. Clearly defined and readily available protocols increase speed of reaction to cyber-attacks.
3. Increased customer / investor confidence, driven by the knowledge that the industry is following a set of commonly agreed upon set of standards.
4. Increased transparency and confidence between institutions.

Feasibility:

1. Initiative design must account for a diverse array of feasible cyber-attack scenarios and a diverse set of organizations and must be continuously improved.
2. Specific standards and controls may vary depending on the type of financial institution.
3. Adoption requires mechanism for enforcing standards (for example, exclusion of members not meeting minimum standards from a network).
4. Potential negative impact on financial institutions unable to meet criteria (for example, a smaller player with less mature cyber-security controls may be subject to sanctions).

II. PARTNERSHIPS

2. CROSS-BORDER AND INTER-SECTOR INSIGHT-SHARING

Challenge:

Defining adequate response and recovery strategies is difficult given the broad scope of potential impacts of large-scale cyber-attacks, including distributed attacks on multiple critical infrastructure industries.

Opportunity:

Cross-border forum for sharing of threat intelligence and cyber-response and recovery best practices before and during a cyber-attack, across critical infrastructure industries, governing bodies, and cyber-threat investigative agencies.

Impact:

1. Improves overall financial services industry preparedness through adoption of best practices from other jurisdictions and sectors.
2. Development of more effective response and recovery approaches that consider role of critical infrastructure providers (for example, cloud service providers).

Feasibility:

1. Cross-border participation may be challenging due to varying data protection legislations across jurisdictions.
2. Significant coordination requirements and limited appetite to distill insights from other industries may hinder successful implementation.
3. Adoption may be challenging as firms are still grappling with determining the appropriate timing and scope of information to comfortably share during a cyber breach.

3. INDUSTRY-COORDINATED DRILLS

Challenge:

Lack of fully effective sector-wide testing may impact the ability of the financial services system as a whole to react effectively during a large-scale cyber-attack with systemic consequences.

Opportunity:

Leverage current industry exercises, such as the Reg SCI test to test, the effectiveness of industry response and recovery capabilities and coordination efforts across financial services and third-party service providers, at a sufficiently granular level.

Impact:

1. Increased speed of reaction to contain the spread and potential impact of cyber-attacks and restore critical financial services operations.
2. Reduced severity of a large-scale cyber-attack, as organizations have more experience disconnecting from affected firms without shutting down business operations.

Feasibility:

1. Difficult to design and agree upon exercises applicable to a variety of financial services and non-financial services players.
2. Significant effort and investment required to mobilize multiple industry participants to run exercises on a periodic basis, especially if international players are included.
3. Limited appetite for conducting real simulations that could cause damage to the financial system.

4. CONTINGENT SERVICE ARRANGEMENTS

Challenge:

Defining adequate response and recovery strategies is difficult given the broad scope of potential impacts of large-scale cyber-attacks (for example, spread to multiple critical infrastructures / subsectors, outage of key players, compromise of backups).

Opportunity:

Arrangements that allow financial institutions to continue critical operations should a partner suffer an outage from a cyber-attack, through partnerships between entities or an industry utility.

Impact:

1. Increased reliability of critical financial services operations and reduced instability and economic gridlock during a large-scale cyber-attack.
2. Reduced potential for contagion by reducing likelihood of a critical player rejoining the financial system prematurely, due to the absence of a substitute service provider.
3. Increased customer and investor confidence, driven by the knowledge that the industry has implemented multiple layers of protection to facilitate continuity of critical industry activities.

Feasibility:

1. Ease of implementation dependent on solution scope (i.e., individual backups vs partnerships vs industry utility). Industry utility and partnership options require standardized format of a large scope of asset classes and are likely more complex to design.
2. Operational complexity and significant monetary and time investment (to allow for continuous testing) render this initiative challenging to design and implement.
3. Potential competitive pressures may hinder adoption (i.e., complete substitutability of a given institution upon short notice would challenge its strategic positioning).

III. UTILITIES

5. WHITE HAT HACKING UTILITY

Challenge:

Lack of fully effective industry-wide testing may impact the ability of the financial services system as a whole to react effectively during a large-scale cyber-attack.

Opportunity:

Utility commissioned to orchestrate and execute large-scale cyber drills.

Impact:

1. Improved knowledge of system vulnerabilities, informing more effective response and recovery procedures.
2. Can help inform improved industry-wide drills.

Feasibility:

1. Complex design, which should incorporate incremental testing to protect existing industry infrastructure from breaking.
2. Likelihood of adoption dependent on risk appetite of financial institutions to engage in live tests that may inadvertently compromise financial services infrastructure.

6. THIRD-PARTY RISK ASSESSMENT

Challenge:

Existing approaches for assessment of third-party cyber resilience create substantial redundancy in the system, as financial services firms each commission their own assessments of the same set of third parties.

Opportunity:

Utility established to assess cyber resilience capabilities of third parties and issue ratings that inform clients as to the adequacy of controls.

Impact:

1. Improved efficiency as assessments of a given third-party can be uniformly leveraged by multiple financial services players.
2. Centralized assessments of third parties could increase usage of more reliable and cyber-resilient third parties.

Feasibility:

1. No major design or production barriers.
2. Adoption dependent on stringency of license requirements; financial services firms may not want to adopt an initiative that restricts their business with critical third parties.
3. Limited benefit from audit of smaller third-party service providers that are unlikely to meet cyber-resilience standards.

7. THREAT INFORMATION-SHARING UTILITY

Challenge:

Detecting the presence of and pinpointing the source of cyberattacks is particularly difficult in the complex interconnected financial system; a sophisticated attack on data integrity can be particularly challenging to diagnose.

Opportunity:

A centralized platform for timely anonymous sharing of threat vulnerability information during a cyber-attack across industries and across borders.

Impact:

1. Faster containment of cyber-attacks from quick dissemination of relevant threat intelligence and defensive measure information, resulting in reduced severity to the system.
2. Increased scope of potential cyber-threats that financial institutions are prepared to respond to.

Feasibility:

1. Cross-border participation may be challenging due to varying data protection legislations across jurisdictions.
2. Adoption may be challenging as firms are still grappling with determining the appropriate timing and scope of information to comfortably share during a cyber breach.

8. DATA REPOSITORY

Challenge:

Defining adequate response and recovery strategies is difficult given the broad scope of potential impacts of large-scale cyber-attacks. While many financial institutions have invested in system and data redundancies, most are not prepared for attacks that could wipe out their back-up systems as well.

Opportunity:

Cross-industry repository and guardian of critical data that provides access as a service to financial institutions (to include data not covered by the Sheltered Harbor facility[8]).

Impact:

1. Provides a layer of protection beyond individual firms' own backups and recovery systems
2. Increased speed of business resumption and recovery, particularly in the case of breaches that have corrupted critical data.

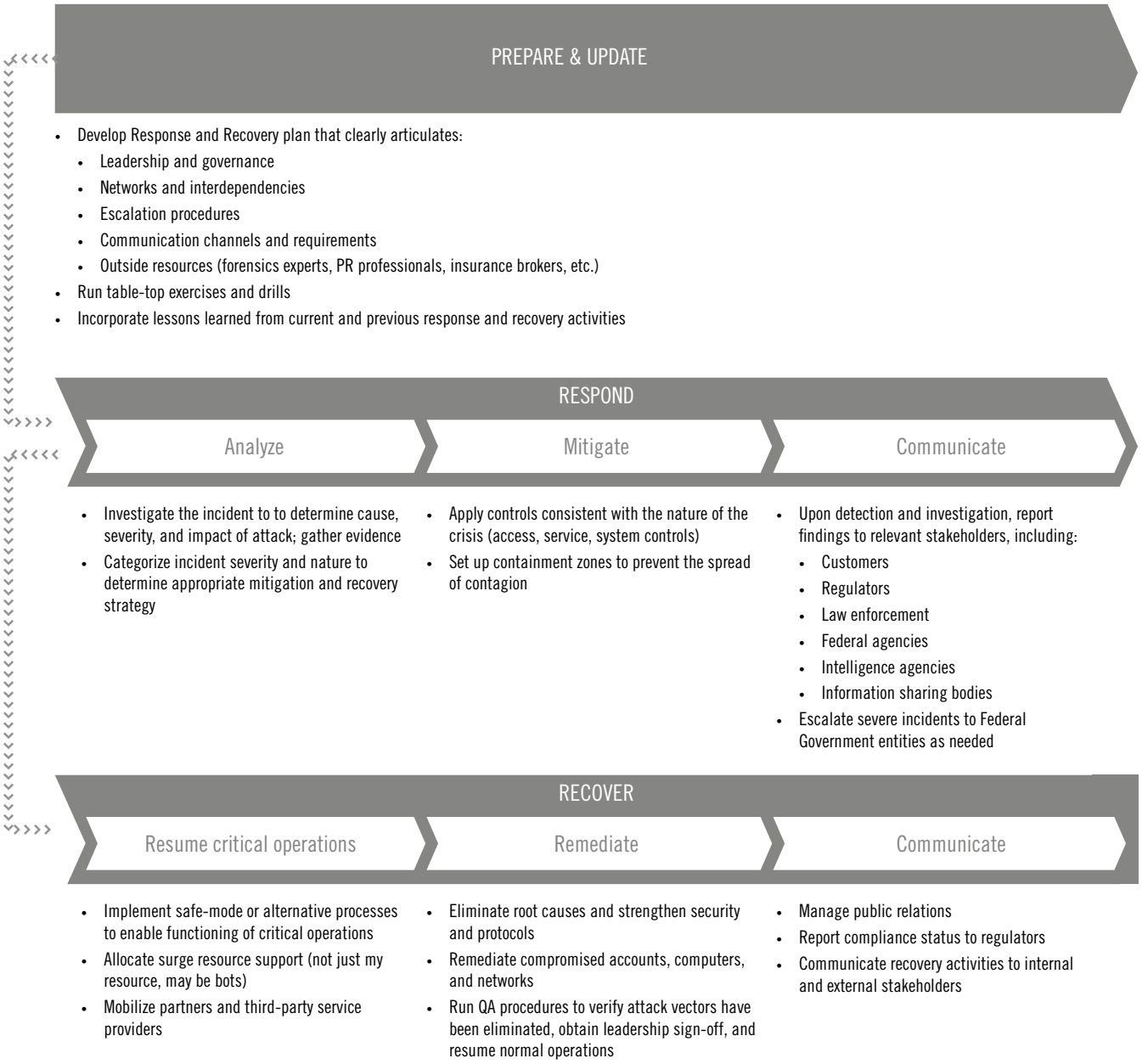
Feasibility:

1. Design of a data repository able to house transaction data from diverse firms requires standardization of data formats and taxonomies, as well as significant data consolidation and encryption investments.
2. Adoption requires trust in the reliability of safekeeping methods and alleviating concerns about competitive pressures, since data processing methods are intellectual property.
3. Continuous testing and maintenance could be very costly.

[8] Sheltered Harbor is a voluntary industry initiative for secure storage and rapid reconstitution of retail bank customer account data. Data is stored in a distributed fashion in a Sheltered Harbor specified data vault, it is kept private by each institution and is encrypted.

APPENDIX B. RESPONSE AND RECOVERY LIFECYCLE

FIGURE 4: RESPONSE AND RECOVERY LIFECYCLE



APPENDIX C. BIBLIOGRAPHY

AIG, "Is Cyber Risk Systemic?", 2017

FINRA. "Report on Cybersecurity practices." February, 2015

Gartner, "Prepare for and Respond to a Business Disruption After an Aggressive Cyberattack," 2017

Harold Gallagher, Wade McMahon, and Ron Morrow, "Cyber Security: Protecting the Resilience of Canada's Financial System," 2014

IMF, "Cyber Risk, Market Failures, and Financial Stability," 2017

Institute of International Finance, "Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system," 2017

OICU-IOSCO and World Federation of Exchanges, "Cyber Crime, Securities Markets and Systemic Risk," 2013

OICU-IOSCO, "Cyber Security in Securities Markets – An International Perspective," 2016

Office of Financial Research, "Cybersecurity and Financial Stability: Risks and Resilience," 2017

World Economic Forum, "Understanding Cyber Risk," 2016

APPENDIX D. ACKNOWLEDGMENTS

CONTRIBUTORS

The project team offers its special gratitude to the contributing organizations for their valuable input in the shaping this study.

Amazon Web Services

Bank of New York Mellon

Citigroup

CLS Group

Depository Trust & Clearing Corporation

Euroclear

Fannie Mae

Financial Industry Regulatory Authority

Financial Systemic Analysis and Resilience Center (FSARC)

Financial Services Information Sharing and Analysis Center (FS-ISAC)

Hewlett Packard Enterprise

JP Morgan Chase

Microsoft

Morgan Stanley

State Street

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

The Clearing House

PROJECT TEAM

The development of this White Paper was supported by combined Oliver Wyman and DTCC project team

Andrew Gray, Group Chief Risk Officer, DTCC

Stephen Scharf, Chief Security Officer, DTCC

David LaFalce, Head of Business Continuity & Crisis Management, DTCC

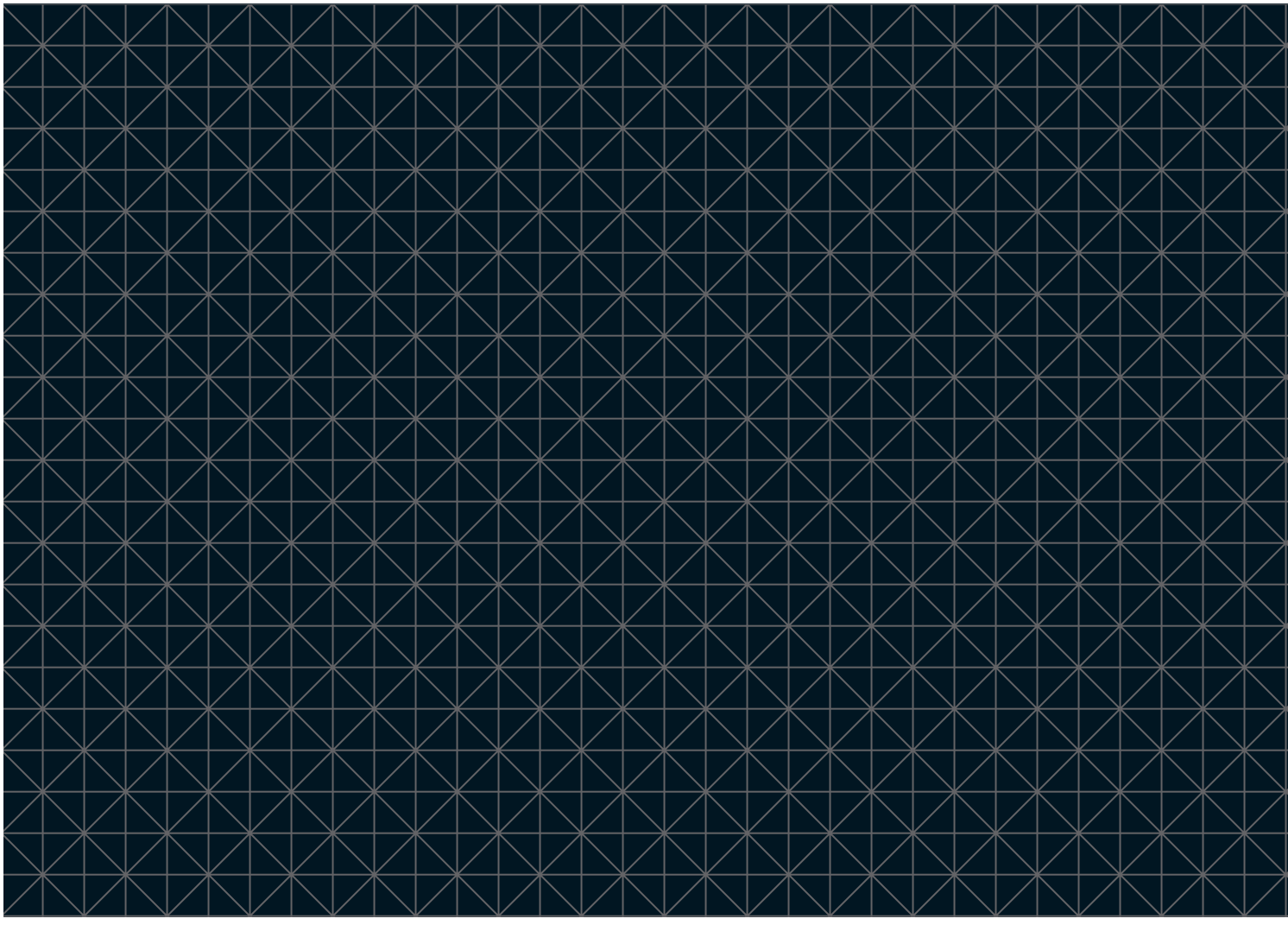
Paul Mee, Partner, Financial Services, Oliver Wyman

Rico Brandenburg, Principal, Financial Services, Oliver Wyman

Desislava Simeonova, Manager, Financial Services, Oliver Wyman

Gabriel Corrochano, Consultant, Financial Services, Oliver Wyman

Questions or comments about this white paper can be addressed to your DTCC Relationship Manager at DTCCClientCommunications@dtcc.com



13918 PS 032018