TLP-AMBER

Mr. Dietrich Domanski
Secretariat General
Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel, Switzerland

GFMA Consultation Response

FSB Public Consultation – Effective Practices for Cyber Incident Response and Recovery
20 July 2020

Dear Sirs and Madams,

Enhancing cyber resilience has been a key element of the Financial Stability Board's ("FSB") work to strengthen financial systems and increase the stability of international financial markets. Given the interconnectedness of the financial sector, in 2018, the Financial Stability Board agreed to develop a toolkit to provide financial institutions with a set of effective practices to respond to and recover from a cyber incident to limit any related financial stability risks.

This work resulted in the April 2020 Consultative Document ("CD") titled *Effective Practices for Cyber Incident Response and Recovery*[1]. The CD provides a toolkit ("Toolkit") to assist organizations in their cyber incident response and recovery ("CIRR") activities. In the CD, the FSB posed a series of questions regarding the CIRR Toolkit, requesting input and feedback from the financial sector.

On behalf of the Global Financial Markets Association ("GFMA"), which consists of the Association for Financial Markets in Europe ("AFME"), the Asian Securities Industry and Financial Markets Association ("ASIFMA") and the Securities Industry and Financial Markets Association ("SIFMA") (collectively, the "Associations"), we welcome the efforts by the FSB and appreciate the opportunity to respond to the CD with input and feedback from our collective Memberships.

In addition to providing responses to the questions in the CD and other comments for consideration, the GFMA has several overarching recommendations that we believe are essential for the FSB to address in connection with finalizing the CIRR Toolkit. In particular, we believe it is critical for the FSB to provide further clarification regarding the proportionality and constructive use of the Toolkit. We also recommend that the FSB use the Toolkit to promote further alignment with existing cybersecurity frameworks. Finally, we believe that the Toolkit should be enhanced to encourage greater uniformity of cyber incident reporting.

Proportionality and Constructive Use of the Toolkit

Financial firms over the years have developed and implemented robust CIRR protocols and controls. To further promote consistency across the sector and reduce regulatory fragmentation, the Financial Services Sector Coordinating Council (FSSCC), GFMA, American Bankers Association (ABA) and Bank Policy / Cyber Risk Institute (BPI/CRI) and other groups developed, in 2018, the Financial Services Sector

[1] FSB, Effective Practices for Cyber Incident Response and Recovery available at: https://www.fsb.org/wp-content/uploads/P200420-1.pdf

Cybersecurity Profile[2] ("Profile"). The Profile is a scalable and extensible assessment tool that financial institutions of all types can use for internal and external (i.e., third-party) cyber risk management and as a mechanism to evidence compliance with various regulatory frameworks globally. The Profile leveraged existing international standards which resulted in 277 controls that align cybersecurity laws, rules, guidance and assessment frameworks from many jurisdictions around the world.

The Profile has since been adopted by over 200 financial institutions of differing sizes and maturity levels. Based on the development and wide use of the Profile, the industry believes its existing CIRR processes and controls are well-developed and are designed to continue to mature as markets evolve.

While the members of our Associations appreciate the need for and purpose of the public sector developed CIRR Toolkit, we respectfully request that the FSB further clarifies that the CIRR Toolkit, as stated within the CD, "does not constitute standards for organizations or their supervisors and is not a prescriptive recommendation for any particular approach." [3] The CD contains other potentially conflicting statements that suggest that the Toolkit can be used by regulatory authorities for supervisory purposes. For instance, the CD states that the Toolkit "may also be useful for authorities as they consider the approaches they may undertake with respect to regulation or supervision, or in responding to a cyber incident within the sector."[4] While financial firms continue to invest heavily in fortifying their cyber defenses, smaller institutions must decide where to invest given limited budgets and staff. The issue being raised here is one of proportionality in that smaller institutions may not be able to implement all 46 CIRR tools at the same level of maturity as a G-SIFI, for example. The FSB should further underscore that the absence of one or more of these practices does not suggest that a financial firm's CIRR program is deficient and is a set of voluntary practices that may be used by financial institutions to enhance their programs.

While we support the use of the Toolkit as CIRR guidance for firms, we believe that the Toolkit should not serve as a basis to regulate or supervise the financial services industry with regard to cyber incidents. Presenting the Toolkit as a comprehensive view to develop regulatory or supervisory standards is contrary to the intent and spirit of the development of the Toolkit and ongoing industry coherence efforts. We therefore recommend that the FSB clarify that the Toolkit is a public sector reflection on industry practices to learn from in coordination with ongoing exercises to further mature CIRR processes and controls.

Promoting Alignment with Existing Frameworks

GFMA continues to believe that more should be done to reduce fragmentation of cybersecurity regulation across the financial services industry. As the FSB highlighted in its important 2017 stocktake of cybersecurity regulations[5], the trend in this area is for further unilateral regulation of cybersecurity practices of financial services firms by national authorities rather than greater coherence. Rather than improving resilience, a globally fragmented cybersecurity regulatory environment for the industry increases financial stability risk by driving complexity into the system. Where regulations relate to the management of incidents or the testing of systems, cross-border coordination is especially important to ensure that resources are not

[2] The Cyber Risk Institute (CRI) is a not-for-profit coalition of financial institutions and trade associations. CRI is working to protect the global economy by enhancing cybersecurity and resiliency through assessment standardization. Its Cyber Profile ("Profile") tool is the benchmark for cyber security and resiliency in the financial services industry.
[3] Consultation at 2
[4] Consultation at 2
[5] FSB, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices available at: https://www.fsb.org/wp-content/uploads/P131017-2.pdf

unnecessarily diverted away from the management of cybersecurity activities such as protecting critical systems.

The Toolkit's 46 CIRR tools correlate closely with practices and controls already established in the financial services sector that are based on frameworks provided by standard-setting bodies such as ISO and NIST, as well as standards from international financial service policymakers such as the Principles for Financial Market Infrastructures (CPMI) by CPMI-IOSCO. The industry fully supports coherence between the Toolkit and these frameworks. The industry notes, for instance, that there has been widespread adoption of the NIST framework globally and that the alignment of the Toolkit with NIST and other existing frameworks is beneficial from an efficiency perspective.

Given the alignment between the Toolkit and existing frameworks, GFMA, along with our other member associations, believe that the FSB should use the Toolkit to further promote the adoption of existing frameworks by national authorities. Greater adoption of existing frameworks by national authorities will help raise the level of cyber resiliency across the industry by facilitating a more uniform use of effective cyber practices by financial firms. GFMA believes that the Toolkit is an optimal place to promote such adoption as many of the tools in the Toolkit are based on these existing frameworks, and their adoption as guidance for firms by the FSB will help spread their use more widely.

As noted above, to help reduce fragmentation, the global financial sector – with input from over 200 banks worldwide - developed the Profile to bring together not just these international standards, but also a catalogue of regulatory and legal framework requirements, to provide a convergence instrument to understand a firm's cybersecurity posture. Work is also underway to integrate, where practicable, emerging guidance from regulatory authorities around Operational Resilience. However, this work is early on as GFMA continues to lead efforts with regulators around the world to work on a coordinated solution. FSB should consider these efforts prior to issuing a final Toolkit to eliminate potential operational and/or cybersecurity resilience fragmentation issues.

The Financial Sector Profile uses a common vernacular that allows supervisors/regulators and the financial services industry to communicate with each other and form a common understanding of a financial firm's cybersecurity posture. It can also be used as a tool for third party cyber risk management and to evidence compliance with regulatory requirements that are based on commonly accepted cybersecurity frameworks.

One way in which the FSB could promote more uniform adoption and use of effective cyber practices is by referencing the Profile in its final document. Because the Profile is based on well-known frameworks such as ISO, CoBIT, NIST and IOSCO cyber resilience guidelines, there is a high degree of consistency between the Toolkit and the Profile which, coupled together, provides the financial industry the best resources available from the public and private sector to tackle cyber incidents effectively. Most recently, both ISO and NIST have engaged international partners in an open, transparent, and collaborative standards development process to develop a technical specification, ISO/IEC 27101[6], on guidance for developing cybersecurity frameworks that leverages the content and approach of the NIST Cybersecurity Framework. In making our recommendation to reference the Profile, the GFMA notes that NIST maps its higher-level framework to ISO 27000, which is designed to enable firms to weave together the technical control focus of NIST with the more risk-driven focus of ISO.

[6] ISO/IEC 27101. Cybersecurity Framework Development Guidelines Draft available at: https://www.iso27001security.com/html/27101.html

Given the complementary value of the Profile to the FSB's CIRR Toolkit, we strongly believe that referencing the Profile could help increase cyber resiliency in the financial services sector by directing firms to a widely regarded and globally used cyber risk management assessment and compliance framework that promotes compliance with the cybersecurity requirements of many jurisdictions. Referencing the Profile could, for instance, enhance transparency and improve compliance across institutions, sub-sectors, third parties, and across sectors, providing a benchmark for regulators to compare cyber resiliency among like financial firms and enabling them to better analyze and mitigate systemic risks related to cyber events. Moreover, use of the Profile by financial firms to demonstrate compliance with regulatory requirements does not preclude ongoing engagement between industry and regulators to address specific areas of concern.

GFMA, on behalf of its global Members, therefore requests that the FSB use the Toolkit to continue to pursue and emphasize its agenda of reducing fragmentation of cybersecurity regulation with national authorities. While we appreciate the need for authorities to maintain flexibility, we believe the current Toolkit could go further in encouraging authorities to adopt more uniform practices based on existing frameworks. In addition to referencing the Profile, another way to do this would be to align the Toolkit's framework, "controls" and lexicon with that of the Profile. Doing so, would relieve financial firms of having to conduct an extensive mapping exercise of this work into firms' existing enterprise governance, risk and compliance (GRC) tools used to manage firmwide risks. The GFMA believes that this step would also help create significant efficiencies not only for firms but for regulatory authorities as well.

Toolkit Enhancement

In addition to the recommendations above, the biggest area where the Toolkit could be enhanced is with regard to cyber incident reporting. Coordination between national authorities is particularly important for cyber incident reporting. The current cyber incident reporting landscape, however, is characterized by fragmentation with differing time, materiality and information reporting requirements among the various national authorities. This greatly increases the complexity and costs for firms as they deal with a multitude of incident reporting requirements while also diverting resources from where they are most needed to address the actual cyber incident.

A recent report from the Bank for International Settlements highlights the scale of the challenge faced by the financial services sector. The report confirms that the financial services faces a higher volume of cyber attacks than other sectors while also finding a positive correlation between the size of an organization and the costs related to the incident. While the authors are not able to reach a level of detail that explains those costs, it is possible that some portion of the costs experienced by larger firms relates to the greater complexity of the regulatory environment in which they operate, including the varying cyber incident reporting requirements to which they are subject. This study suggests that more should be done to understand the regulatory costs faced by large firms in connection with cyber incidents and ways in which these costs and the associated complexity can be reduced to the extent they result from non-uniform incident reporting requirements.

Accordingly, GFMA strongly encourages the FSB to use the Toolkit to promote greater uniformity in cyber incident reporting requirements, which should help reduce the unduly burdensome demands that firms face today. Greater uniformity will allow firms to keep authorities properly informed of cyber incidents while also providing them more time and resources to deal with actual incidents.

Previous studies by the FSSCC have shown that nearly 40% of critical cyber staff are tied up dealing with overlapping and sometimes conflicting reporting and other requirements rather than being on the front-lines protecting the firm or building more robust cyber capabilities. Given the significant concern regarding this issue among the GFMA Membership, GFMA also strongly encourages the FSB, as a next step in maturing cyber resilience, to consider creating a separate workstream focused on promoting uniformity among the various jurisdictions regarding cyber incident reporting requirements.

The industry believes that a comprehensive and consistent incident reporting framework would serve as a foundational component to increase efficiency of sector-wide coordination during an incident with peers and regulators. Only a common and consistent incident reporting framework will allow incident data to be aggregated and analyzed in a time-critical manner for public-private real-time collaboration between regulators, supervisors, law enforcement, financial firms and other critical infrastructures.

In addition, GFMA recommends linking such a comprehensive harmonized incident reporting framework with a common taxonomy of incidents, based on relevant international standards. Such a taxonomy should be comprehensive, to include various cyber and other operational disruptions, but also flexible in nature to evolve over time.

Our collective Memberships further agree that such an incident reporting framework should encompass only significant security incidents, based on common materiality thresholds, to avoid firms having to report on all cyber incidents whether they are material or not. Common materiality thresholds should be proportionate/risk-based to be flexible and applicable to firms of various sizes/types.

* * * * *

In addition to these overarching recommendations, GFMA is providing in the attached document specific responses to each of the questions put forward in the CD. GFMA notes in particular that, with regard to the governance discussion in the Toolkit, recovery point objectives (RPO) and recovery time objectives (RTO) are important metrics for an organization. However, it would be counter-productive to mandate one cyber baseline RTO / RPO for all organizations – nor is there one universal threshold for the severity of incidents to be reported. The severity and recovery objectives for incidents can vary greatly, based on the nature and impact of the unique threat, as do the dependencies and structures of the organizations themselves.

Overall, we believe that adoption of the recommendations above will go a long way toward increasing the utility of the Toolkit. Moreover, given the high degree of conformity between the Toolkit and the Profile, as an industry, we would like to begin a dialog to ensure the FSB is comfortable with the use of the Profile to demonstrate compliance with cybersecurity requirements of national authorities.

We also look forward to working with FSB in development of a taxonomy on incident reporting. The work undertaken by the FSB, such as the creation of the Cyber Lexicon, acknowledges the importance of language and its ability to affect positive change. Language helps link a wide swath of our shared cultures and values and must evolve alongside these constructs – whether passively or actively.

Amidst increasing social awareness of inequality and racism pervasively present worldwide, positive change is needed to ensure we shape a better and fairer future than the present. Just as regulators and standard-setters consider potential impacts that new technologies may have on bias, discrimination and financial

exclusion, so too should we explore how language within our industry shared may implicitly support racially insensitive stereotypes.

We welcome the FSB and its peers to join market participants in this effort, and to encourage the altering of any standards' language which may carry such negative connotations wherever identified. This includes terms such as "whitelisting" and "blacklisting", or "master" and "slave" servers, among others. Although the FSB itself has not employed any of these terms in neither this consultation nor the Lexicon, we would be grateful if you joined us in encouraging regulators and market participants to strive for more equitable language going forward.

We recognize the evolution of markets and with each event industry and regulators learn new factors to take into consideration. We value and welcome ongoing collaboration and engagement on these matters. We also are more than happy to be an industry resource to facilitate feedback for questions the FSB has regarding the financial services sector's cybersecurity posture and overall resiliency during extreme events.

Respectfully,

Allison Parent
Executive Director
Global Financial Markets Association
www.gfma.org

Questions for Public Consultation – Industry Reponses

General

1.1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?

- During COVID-19, the financial firms and government agencies experienced, as is usual during major disasters, an increase in COVID-related phishing and business email compromise schemes, credential stuffing, malware, ransomware and denial of service attacks as well as incidences of financial fraud against unemployment systems, stimulus payments and websites selling defective Personal Protection Equipment (PPE).
- Financial firms are well prepared for these types of events given the significant cyber security investments made over time and the level of preparation and testing conducted by business continuity and crisis managers at each financial firm. Even given the extreme nature of this event and significant swings in market volumes and volatility, the financial sector showed significant resilience – the global markets operated well, the major global equity, fixed income and derivatives exchanges performed without incident and trades cleared and settled timely without any major failures across the sector or individual financial firms.
- Cyber incident response teams are typically geographically dispersed and, as such, this directly contributed to being able to shift to remote work seamlessly. Moreover, cyber incident response processes overall operated as designed at financial firms around the globe with no major issues reported during these unprecedented times.
    - However, with the unique work from home (WFH) situation imposed on a large number of users across the organizations, cyber incident reporting and response procedures needed some adjustment given the resources available and the scope of the cyber incidents have widened to cover devices owned or deployed at the end user homes.
- While the current situation is unprecedented in many respects, the plans, processes, and tools the firm already had in place to protect against a disruptive cyber event are working as planned. Given that in the industry more than 90% of employees worked from home, financial firm network and IT infrastructure proved it can support mission-critical and essential workers, as well as administrative users, for long periods of time. While the WFH access methods used uncovered some minor improvements firms could make to the resiliency of the infrastructure, all have contributed to make a firm a more stable organization. Financial firms are also taking the following steps, which are repeatable for future events:
    - increasing infrastructure capacity for remote workforce and enhanced alerting capabilities to detect potentially malicious access attempts
    - enhancing specific controls to safeguard remote access sessions, such as detections to identify brute-force login attempts and preventative controls to block users from copying firm information onto personal devices
    - reinforcing baseline security practices for the remote workforce including targeted messaging to users to remind them of policies or special entitlements
    - maintaining transparent and proactive communications with vendors to meet both risk management and regulatory requirements and ensured business continuity processes (BCP) with critical vendors in the event of an incident.
    - reviewing and confirmed Distributed Denial of Service (DDOS) mitigation plans, particularly for the remote login infrastructure

- updating long-term enterprise security strategies and policies for firms and third parties to ensure appropriate coverage in the event of a second or third wave or another contingency event similar to COVID-19
- monitoring for additional DLP and security exposures
- performing real-time, ongoing, organization-wide remote workforce testing
- strengthening security controls for existing digital services (e.g. VPN infrastructure)
- strengthening awareness initiatives regarding cyber risks related to the pandemic

1.2. To whom do you think this document should be addressed within your organization?

- Global, Deputy and Departmental CISOs
- Chief Information Officers
- Enterprise and Operational Risk Officers
- Cybersecurity Operations Teams (SOC, CSIRT and CERT)
- Cyber, BCP and IT Incident Teams
- Cyber Fusion Center Heads
- Corporate communications
- Control Functions (risk, compliance, audit)
- Legal, Compliance and Privacy

1.3. How does your organization link cyber incident response and recovery with the organization's business? Does your organization follow international standards or common frameworks? If so, which international standards or common frameworks?

- First of all, with regard to the connection of the response and recovery activity to the business of the organization, as soon as CSIRT receives the report relating to the current critical event, it contacts and engages all the structures concerned by the event to understand its severity. Once the necessary preliminary information has been collected, it convenes a first alignment meeting involving all the necessary entities for the management of the event. The constant involvement of the business also allows it to be kept aligned on the evolution of the event and the possible impacts.
- Financial firms also naturally link their cyber incident response and recovery to the overall business. Cybersecurity is a key resource leveraged as part of the enterprise incident response to both inform and react to enterprise events. Within the financial industry there is a criticality and importance placed on holistic incident response capabilities that supports the restoration and recovery of the business – this is the primary focus. Cyber incident response is a major component to that process. If a business application is affected by a cyber incident, the response teams will make it a top priority to do several things: 1) properly communicate to all affected and involved parties; 2) recover such that the application's stability and security are restored with no adverse effect to the firm; and 3) conduct a "lessons learned" session to best defend against a repeat scenario.
- Financial firms typically maintain a dedicated cybersecurity program responsible for protecting the confidentiality, integrity and availability of firm resources. The firm's cybersecurity program also contains a firmwide cyber incident response framework that outlines the processes and guidance for how the firm responds to and recovers from cyber incidents. Financial firms have designated cyber incident coordinators across the firm's divisions and maintains division or business-specific response and recovery guidelines and processes tailored to the specific commercial, regulatory, and legal requirements of the firm's lines of business.

- Cyber Incident and Response is also a part of IT Incident management processes for those cyber events that impact the technical IT infrastructure (e.g., operating systems, applications, systems, networks etc.). Depending on severity and business impact, for example, a cyber incident also would roll up to a firm's Crisis Management Team that is business linked and owned by CxO-level executives and in extreme cases, the firm's Board of Directors.
- In the event of a security incident, firms have also developed processes that engage both data privacy and business continuity departments. Data Privacy is involved to ensure compliance with local and regional data privacy regulations, and for legally required notifications in cases of data compromise. Business continuity is engaged in cases where events may cause disruption to business-critical services. Those critical services are defined by the key stakeholders within critical business units.
- Financial firm incident response processes have been built leveraging best practices identified in the MITRE Attack framework, The NIST Framework for Improving Critical Infrastructure Cybersecurity and SP 800-53 for establishing Security Controls, COBIT, ISO 2702, ISO/IEC 27001, SOC2, GDPR, and other internationally recognized standards. Financial firms are also rapidly adopting the NIST-based "Financial Sector Profile" which incorporates and harmonizes the above set of standards as well as global cybersecurity regulatory rules, regulations and guidance into an integrated set of cybersecurity controls.

1.4. Does your organization structure its cyber incident response and recovery activities along the seven components set out in the FSB Toolkit? Please describe any additional components your organization considers.

- While not directly, financial firms leverage and have adopted activities and controls that parallel the seven components of the FSB Toolkit (Governance, Preparation, Analysis, Mitigation, Restoration, Improvement, and Coordination/Communication). Financial firm Incident Response process are also tied into the overall Enterprise Incident Management process that leverages cross divisional coordination and communication practices to ensure rapid response to incidents. Financial firm business teams are key partners in these efforts by helping to assess impact, recovery, and communication efforts to key stakeholders
- Cyber incident response and recovery activities are structured on the basis of the seven components indicated in the FSB Toolkit. In particular:
    - The definition of tasks and responsibilities within the company regulation (tools 3 and 9).
    - The definition of a runbook for the management of possible event scenarios (tool 10), and a set of communication templates to be used (tool 11) are being addressed within the organization.
    - The definition of cyber incidents taxonomy that contributes to a rapid and homogeneous classification of events at corporate level (tool 19).
    - Once a critical event has been identified, the coordination of activities by CSIRT towards all involved functions, aimed at mitigating the effects of the event itself (tools 22-25) and identifying recovery actions (tools 26-33).
    - The tracking of lessons learned and possible improvements in the management of specific events (tool 40).
    - The information sharing always carried out reliably and quickly (tool 44) to guarantee a timely escalation within the organization for the management of events (tool 41).
    - Finally, the periodic and continuous alignment meetings on the event with CSIRT and involved functions to provide regular updates on the evolution of the activities, and actionable, accurate, timely and concrete information (tool 42).
    -
- As noted above, many financial firms are adopting the NIST-based set of controls built into the "Sector Profile" whose controls are very closely matched to the FSB Toolkit.

1.5 **Based on your organization's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).**

- **Governance** – (3, 5) Firms have established a strong corporate culture regarding security and risk within their organizations which aids in all of the coordination of activities in responding to CIRR. Roles and Responsibilities are defined across the organization to ensure that decisions are made quickly and effectively as determined by the severity of the incident.
- **Preparation** – (10) The key component of a firm's capability to react to cyber incidents is a fully documented Incident Response Plan that details all of the necessary information included within the FSB toolkit.
- **Analysis** – (20, 21) Robust access is necessary to logs, SIEM data and other sources of information that can highlight the event that relate to the impacted systems and services.
- **Mitigation** – (22, 23) Containing the impact of the cyber incident is the main priority. Leveraging existing Business Continuity framework where possible will aid the business in ensuring that the damage or loss is minimized.
- **Restoration & Improvement** – (33) Firms maintain Gold Copy versions of their system configurations that allow them to detect and react to deviations from the standard, as well as recover damaged system configurations in the event of corruption, degradation, or failure.
- **Improvement** – (34) In addition to cooperation with Business Continuity Team exercises, firms also conduct periodic tests of incident response, alternate workspace, and communications processes multiple times per year. In many cases, Scenario-Based Reactional Tests (SBRT) are performed to exercise skills and tools with the SOC and other cyber security teams.
- **Coordination & Communication** – (41, 42) Timely identification and escalation of cyber incidents and threats are paramount to minimizing the damage from a cyber incident. This, coupled with regular updates to key stakeholders, as defined by the playbooks and Incident Response processes, will ensure that communication is coordinated and appropriate.

1.6 Based on your organization's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).

- Box 1: Metrics – Firms generally track metrics similar to those listed in Box 1 as well as industry standard metrics that indicate availability, duration, potential lost revenue and service level performance of their internal cyber teams as well as external service partners. These metrics need to be articulated in a consumable manner, typically customized dashboards, to relevant stakeholders across the organization.

- Box 2: Stakeholders – Financial firm existing Incident Response Plans and playbooks communicate to appropriate stakeholders, internal and external contacts, and relevant other authorities to be engaged during a cyber incident response. Firms also adhere to regulatory reporting requirements for significant events whose form and content varies substantially across the regulatory community. The most relevant and/or telling of these metrics will be shared periodically with the Board the Directors, which is made up of relevant stakeholders from across the firm inside and outside the institution. This allows the organization to make informed, consensus decisions based on the metrics provided and different risk management perspectives.

- Box 3: Taxonomy: Financial firms generally leverage industry standard classification, documentation, and severity definitions for all cyber incidents.

- Box 4: Scope and Type of Tests – Scenario-based testing of firms Cybersecurity Operations Center, Incident Response processes are continuously exercised to identify strengths and gaps in process, skills, and data access in order to shape improvement efforts. Financial firms test resilience as a part of business-as-usual operations rather than as part of a discrete, episodic testing regime.
    - Financial firms also approach red teaming and penetration testing by hiring suppliers have no knowledge of a firm's network and its underlying infrastructure and architecture to perform this function on an annual basis. Firms receive valuable results from this approach since suppliers

change their tactics and style of attack each time based on the current and emerging risks gleaned from the intelligence community.
    - While tests like penetration-testing and red-teaming are important aspects of a robust cybersecurity program regulators should not seek to conduct these tests themselves on institutions or dictate specific methodologies or vendors for institutions to use. Instead, institutions should be expected to make risk-based decisions on what vendors to use, including being able to use its own testing team as necessary.
    - Some regulators mandate that firms must use a third-party to conduct testing. However, firms with the capability to conduct a firm-led test should have the option to conduct testing on its own environment using its own testing teams. Not only is testing less risky, but firm-led tests have the advantage of being able to conduct more thorough tests than a third-party provider who could be limited by knowledge and liability.
    - Likewise, we seek to limit regulatory access to take custody of data related to cybersecurity vulnerabilities. For example, attack simulation results can be highly-detailed reports of the vulnerabilities in certain technologies or the weakness in a network system, or security program. In the wrong hands, these reports are a useful map for a cyber-attack.

- Box 5: Shared Information – Non-specific threat intelligence that does not directly align to specific corporate attacks to an organization and may address a broader sector of the industry will be shared with Law Enforcement or other authorities and agencies as appropriate. An effective practice firms have found is to share top of mind threat intelligence curated by their cyber threat intel teams with our law enforcement and government partners. Firms typically schedule quarterly meetings with their public sector and law enforcement partners to share threat intelligence. In return, those organizations share back defensive recommendations as well as validation as to whether the threat intelligence firms have curated is accurate.

- Box 6: Information in Cyber Reporting – Any details of a threat or attack vector that does not provide specific details related to direct losses or attacks against an enterprise might be shared. This would include the Type of Incident, Indicators of Compromise (IOCs), and general information regarding the target of the attacks, and potential mitigation and remediation actions that could be taken.

1.7. What role, if any, should authorities play in supporting an organization's cyber incident response and recovery activities?

- Authorities should play both a Threat Intelligence role, advising organization of immediate or upcoming threats to the organization or wider industry. In addition, regulatory authorities can play a supporting role to help investigate a cyber incident when requested by the organization. More importantly, authorities can serve as an escalation path for intelligence and prosecution.
    - However, a single incident might entail the need to report to different Supervisory Authorities complying with different regulations; all these different criteria and patterns cause fragmentation with respect to the overall incident reporting requirements and can subtract resources from the handling of the incident itself. At this regard, it would be helpful for the different authorities to cooperate for a clear set of consistent shared requirements and standards.
- Authorities should also disseminate timely and actionable threat intelligence to inform firms of specific threat actors of concern and share effective risk management and mitigation practices. Additionally, authorities should be able to deploy capabilities to assist firms in response to "significant" cyber incidents in support of affected firms' incident response activities.
- CIRR processes may include alerting the authorities that an incident has occurred for awareness but can include a joint investigation. The authorities have the ability to provide insight and can bring additional resources and intelligence for accurate incident resolution. The authorities, in this role, can be a tremendous asset to the industry.

- Consistency between regulators and "proportionality" is important to minimize regulatory overhead depending on a firm's presence in particular jurisdictions. Along these lines, use of a common lexicon, taxonomy and consistent regulatory reporting data requirements across regulatory bodies is of paramount importance to increase efficiencies.

1. Governance

1.1. To what extent does your organization designate roles and responsibilities as described in Tool 3? Does your organization identify these roles by business line, technology application or department?

- Based on the specific nature of the incident and its severity, the involvement of the different competent functions is assessed, and all the identified stakeholders are included in periodic alignment meetings throughout the incident management evolution and the recovery activities definition.
- Financial firms also maintain an incident response program documented in a written framework, with clearly defined roles, responsibilities and levels of decision-making authority. These roles are primarily delineated by business division but are complemented by subordinate division-specific incident managers and incident response coordinators. Designated members of management are held accountable for implementing and managing the cybersecurity program, which includes governance for cyber incident response.
- Criteria have been established for escalating cyber incidents or vulnerabilities to senior management based on the potential impact and criticality of the risk. Empowerment of the manager (or supervisor) or leader to take the appropriate action to "act to shift behavioral norms to mitigate cultural drivers of misconduct". These roles are not identified by business line, technology application or department.
- In many financial firms, the Head of Cybersecurity Operations is the "Incident Owner" for all cyber related issues. During an event and depending on the sensitivity of the issue, the incident owner will be appointed to capture relevant notes, timelines, data forensics, and other materials relevant to the incident investigation and remediation activity.
- Developing playbooks for scenarios is essential to ensuring the right stakeholders are involved at the outset when responding to that class of cyber incident and typically include the following teams:
  - Crisis Management
  - Incident Oversight
  - Cyber, BCP and IT Incident Management
  - Computer Security Incident Response Team
  - Containment and Remediation Teams
  - Legal Counsel
  - Corporate Communications
  - Others

1.2. How does your organization promote a non-punitive culture to avoid "too little too late" failures and accelerate information sharing and CIRR activities?

- Financial firms promote a top down culture of "escalation," which encourages all employees to notify superiors or designated personnel of operational and other business risks. This culture is reinforced through in-person training for new hires and supervisors, and mandatory annual online training for all firm personnel. Online training includes modules that outline best practices for incident reporting and scenario-based questions, which encourages firm personnel to report operational risk events regardless of whether they meet the minimum reportable thresholds. These activities are codified in a written policy and standard which establish the minimum reporting requirements and thresholds for the firm. Firms conduct periodic "just in time" cyber and information security training on specific risks for high risk groups. This collaborative approach where everyone's ideas/opinions/perspectives are respected & valued has led to quicker resolution times and stronger bonds between various incident response teams. In year's past, employees were

sometimes reticent to declare an incident because it would pull in many resources, including stakeholders and executives to triage the incident. But by doing so, with an incident comes the need for immediate changes and concurrent approval to do so. Having leadership/stakeholders/executives engaged up front offered expeditious approval to make the changes. This too improved resolution times.

- Financial firms have also developed a strong Cybersecurity Awareness culture where they constantly stress the importance of early warning of cyber issues. Extensive phishing testing, awareness campaigns, corporate intranet articles, and hotlines to report issues has created an environment where employees feel comfortable identifying and escalating suspicious activity or events to security teams. This promotes a very healthy culture; a key value being "Doing the Right Thing"
- Firms also stage Information Security Awareness/Education programs to ensure all members or staff know how to and when to report any suspicious activity. As well as clearly describing staffs expected roles and responsibilities within the organizations policy's, standards and procedures.
- Empowerment of the manager (or supervisor) or leader to take fair but appropriate action is important. More often than not a verbal discussion over the matter will suffice. Fairness is stressed across the team along with lessons learned so actions leading to incidents are not repeated.

2. Preparation

2.1. What tools and processes does your organization have to deploy during the first days of a cyber incident?

- Financial firms coordinate incident handling activities with contingency planning activities; that
  - identifies essential missions and business functions and associated contingency requirements
  - provides recovery objectives, restoration priorities, and metrics
  - addresses contingency roles, responsibilities, assigned individuals with contact information
  - addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure
  - ensures eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented
- Many organizations typically adopt an incident management group process that allows, based on the specificity and severity of the incident, to activate the appropriate internal escalation and decision-making process leading, if necessary, to the activation of the crisis management model. These practices allow not only the correct coordination and internal collaboration but also the fulfillment of reporting obligations to the competent authorities in an effective and efficient way. The most suitable strategy is defined on the basis of the information, promptly and accurately collected, and the impacted processes.
- Cyber events/incidents are typically managed through an Incident Response Framework. Specifically, in response to a Cyber Event, defined here as any cyber threat, vulnerability, and/or cyber incident that introduces cyber risk to the firm, the Incident Management Team, in coordination with the firm's Chief Information Security Officer (CISO), rapidly convenes a meeting of subject matter experts to assess the level of Cyber Risk (CR) and determine the most appropriate avenue for response.
- The following is a non-exhaustive list of tools and processes firms deploy during an incident:
  - CIRT – playbooks, priorities, ticketing systems, forensics and triage
  - 24/7 SOC,
  - Incident Response Playbooks,
  - Major Incident Response Playbooks,
  - 3rd Party Incident Response Retainers.
  - BCP Plans.
  - Third Party threat Intelligence.
  - Forensic Tools
  - SOC, Technology solutions and vendors

  - ServiceNow Cyber Incident Response
  - MITRE Attack framework
- Firms also leverage Third-Party Best Practice tools as typically identified by professional firms such as Gartner Magic Quadrant, Forrester, or other technology ranking companies

2.2. Please provide an example of how your organization has enhanced its cyber incident response plan over the last 12 months.

- Financial firm cyber incident response plans and associated processes are constantly evaluated and updated with lessons learned from both real-world incidents as well as assurance testing and tabletop exercises. In addition, firms:
  - Developed measures of performance and effectiveness that help them continuously improve efficiency in managing cyber incidents and events.
  - Participated in numerous internal and external exercises with peers and government partners which provide a fresh perspective on cybersecurity tools, threat drivers and industry response
  - Replaced SOC vendor and ticketing system which now has more contextual info (pre-fetch information for analysts).
  - Enhanced monitoring, detection and response capabilities, updated plans and playbooks.
  - Defined categories of incidents, and prepared detailed runbook processes for each type of possible incidents.
  - Worked closely with the Business Continuity organization to ensure alignment with a cyber incident response with a "Work from Home" contingency plan, particularly if an attack is targeted at remote connectivity infrastructure.
  - Participated in the Quantum Dawn exercise in November 2019. The exercise dealt with adversarial action within one firm across multiple countries/geographies. With regulators from different countries participating, we realized they have different rules/expectations on when they are to be notified of a major incident. The playbook dealt with one-country-model.
  - Updated the rules for the business continuity plans to include all possible scenarios and enhance cyber events
  - Updated processes for critical event management
  - Reviewed and update of the crisis management model
  - Started a "critical event readiness" project for the identification and formalization of contingency solutions relating to the organization's digital services
  - Participated in external cyber exercises (e.g. G7 Simulation for Cross-border Coordination) and internal crisis simulation (table-top exercises
  - Re-organized segregation of tasks between the event's phases of classification, management, mitigation and lessons learned, analysis, intelligence.

- Financial firms have also developed "Virtual Fusion Centers" to quickly and efficiently responds to cyber related incidents and events. By leveraging existing processes, teams and budgets, a Virtual Fusion Center will converge the identification and escalation paths into a central incident management process. The centralized incident management group will enhance the effectiveness of the firm's existing incident management processes. The Virtual Fusion Center will consistently:
  - Coordinate integrated escalations to regional, divisional, and global leadership
  - Ensure various regulatory, contractual, and legal aspects of an incident are identified and addressed
  - Determine the root causes of the incident then propose and manage effective remediation
  - Execute, or enable the execution of, notification requirements to regulators and clients
  - Serve as a center of knowledge for incident management, through recurring exercises to promote further integration across incident response functions
  - Promote efficient communication through appropriate channels and consistent, timely messaging

2.3. How does your organization monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?

- Financial firms over time have implemented robust global Third-Party Risk Management programs, processes and tools. These programs provide a globally consistent governance framework to risk assess third party service providers prior to engagement and for the ongoing oversight, monitoring and review of the service providers following on-boarding. Depending on risk, sensitivity of data shared, and/or criticality of the third-party process to the business, for all third-party suppliers, firms require completion of an initial risk questionnaire by the candidate supplier that will provide insights into potential risk areas. In critical, high-risk, or suppliers handling sensitive data (PII), an onsite visit to the third-party supplier may also be undertaken to evaluate their data and security controls. Risks and outcomes are captured and reported back to the business owner and periodic reviews are undertaken to ensure continued compliance with internal security requirements.
- The programs also lays out guidelines for assessing the risk associated with each vendor, including reviews that evaluate information security, business continuity, regulatory, sub-contractor, reputational, financial, geo-political, and business criticality risks. Firms also maintains a subordinate vendor technology risk program, which assesses the data, technology (i.e. security, cloud, cyber, web and mobile applications etc.), and continuity risk posed by vendors and establishes a process to ensure vendors have appropriate controls in place. This includes coordinating risk assessments of third-party service providers, defining minimum cybersecurity practices to be met by such providers
- Firms also conduct periodic review of regular KRI/KPI reported by 3rd parties and business lines. Additionally, service providers are subjected to continual vendor risk assessments and onsite audits as necessary.
- Many firms have also established Quarterly Business Reviews (QBRs) and Executive Business Councils (EBCs) with critical third-party service providers.

3. Analysis

3.1. Could you share your organization's cyber incident analysis taxonomy and severity framework?

- Financial firms use several existing taxonomies and frameworks today:
    - The MITRE Attack Framework
    - Fusion Cyber Risk Scoring Methodology – Critical/High/Moderate/Low/None based on Maturity of Attack, Threat, Complexity of Response, Impact, Vulnerability and Controls
    - CIRT Security Incident Risk Ranking – Critical/High/Low based on Impact to Systems and Services, Loss, Regulator Action or Reputational Damage
    - Categories as defined by US-CERT (https://www.us-cert.gov/government-users/reporting-requirements)
    - ITIL Incident Management guidelines for process and severity frameworks

3.2. What are the inputs that would be required to facilitate the analysis of a cyber incident?

- The timely collection of information relating to the impact perimeter (which/how many devices, tools and/or systems involved) and its severity concerning reputation, regulations and economic effects, and the promptness of such information allow to start the analysis of the incident and define the appropriate response action. Typical inputs to a cyber incident taxonomy would include:
    - Incident Title
    - Event Class + Event Type
    - Current Status of the Incident Response (Open/In-progress/Resolved/Closed)
    - Impact Level (RL 1/ RL 2/ RL 3/ None)

- Incident ID
- Incident Reported time
- Incident Description
- Action Taken
- Incident Resolved time
- Incident Closed time
- Pending/Follow-up actions
- Overall Impact Level
- Business Impact
- Technical Impact
- Trigger Point
- Infection Vector
- Vulnerability Management
- Malware Analysis
- Threat Actor
- Targeted against the firm
- RFI with threat partners
- Actions Taken
- Controls that failed
- Controls that worked as expected
- Offending IOCs
- New/predicted/standard style of attack
- Targeted infrastructure
  Communication with adversary
- Time down
- Anomalous or malicious behavior detected & alerted
- Additional controls if above control failed

- The CIRT Procedures Runbook also provides general guidance or checklist on handling an incident. Actions in the checklist include Detection and Analysis:
  - Determine whether an incident has occurred
  - Analyze the precursors and indications
  - Look for correlating information
  - Perform research (e.g., search engines, knowledge base)
  - Document the investigation and evidence gathering
  - Classify the incident using the incident categories
  - Follow the appropriate incident category checklist
- Financial firms capture security events relating to Endpoint, Server and Directory Services and Network Level Monitoring, events from all Security Controls (Firewalls, AV Agents etc.) as well as Logs and alert output from SIEM tools and IT systems
  1. Contact information for the reporting site and any other parties communicating in response to the incident.
  2. Names and network addresses of hosts involved in the incident.
  3. The nature of the activity.
  4. Description of the activity and relevant information (such as logs, associated time-zone information and other artefacts).
  5. Tracking/ticket numbers that may have already been assigned (by a local or regional helpdesk, security team/SOC/NOC).
  6. Confirmation if activity/incident is related to recent change request.
  7. Names of the business units currently being impacted.
  - Whether there is potential for impact on external parties (clients, vendors etc.).

3.3. What additional tools could be useful to analyze the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?

- Implementation of tools that solve the challenges of managing multiple and fragmented requirements in an efficient mandatory incident reporting process, and the implementation of prevention and monitoring tools in order to limit the risk of the incident occurring.
- Establishment of a shared database including all cyber incidents and the possible root cause of these incidents would be useful.
- Robust suite COTS products that expand a Defense in Depth strategy and provide actionable data to quickly identify and resolve security incidents. These tools include robust Data Analytics, SIEM, ticketing systems, all of which we have deployed to an enterprise
- Tools that automatically build trends and relationships, if any, between cyber incidents.
- Effective tracking and reporting matrix that could include time to resolve in each steps of the incident.
- Incident Response metrics and data analytics
- Incident Lesson Learnt procedures
- Incident Remediation reviews
- Control effectiveness exercises
- Tabletop exercises
- Pen Testing and Red Teaming

3.4. What sector associations does your organization participate in and what benefit does your organization accrue from that participation?

- AFME, ASIFMA, SIFMA
- Bank Policy Institute
- CERTFin and ABI (Italian Banks Association)
- Cyber Defense Alliance (UK)
- Cyber Security Intelligence Group (CSIG)
- EBF
- ESCO
- Federal Bureau of Investigation (FBI)
- FCA Cyber Coordination Group
- FS-ISAC – Information sharing, specifically threat intelligence from peers/financial institutions.
- FSARC- Financial Systemic Analysis & Resilience Center
- FSSCC – Classified threat intelligence briefings and ability to influence cyber policy directly with the Department of Treasury and Department of Homeland Security.
- Institute of International Finance (IIF)
- InfraGard
- Monetary Authority of Singapore / Association of Banks in Singapore
- NCA
- National Cyber Forensics and Training Alliance (NCFTA)
- National Cyber Security Centre (GCHQ)
- U.S. Department of Homeland Security (DHS/CISA)
- The Department of the Treasury
- The National Cyber-Forensics and Training Alliance (NCFTA)

4. Mitigation

4.1. Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?

- Speed to recover
- Impacts on the business processes due to Incident containment measures
- Impacts to the markets and downstream financial ecosystem
- Data confidentiality, integrity and availability
- Impacts to third and fourth parties
- Impacts to Business Continuity Plans
- Internal and External Communication Plans.
- Incident Logging
- Regulatory, Compliance and Legal Risks and Reporting
- Human resources
- Reputational risk exposure
- Firm financial and economic impacts
- Consumer impacts
- A full accounting of response and mitigation activities

4.2. What tools or effective practices does your organization have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?

- Tools with contingency measures (IT, Operational and Communication) to guarantee the continuity of customer service, and to mitigate any regulatory and reputational impacts deriving from cyber and/or business continuity incidents to guarantee the continuity of digital service.
- Defense in depth involving policies, permissions, and data controls help mitigate risk from cyber incidents. Additionally, all cyber incidents automatically notify interested parties based on region, data type, entity, business/ division, and impact
- Incident response plan designed to enable recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cybersecurity incident
- Continual testing of systems, applications, and data recovery procedures
- Testing of information backups periodically to verify they are accessible and readable
- Annual testing of business continuity and resiliency plans
- Ensuring critical online systems and processes are tested to withstand stresses for extended periods
- Comprehensive monitoring of data loss controls
- Incident Response Playbooks and Containment/Isolation Plans. Major Incident Plans
- Data Privacy Major Incident Response Plans
- DLP Tools and Monitoring
- BCP Plans
- Access Control Systems
- Network Segmentation
- Information Security Awareness/Education.
- Contracted services for penetration testing & vulnerability assessment
- Security Incident and Event Monitoring
- Contracted Threat Intelligence services
- Hardened client and server builds

- Anti-Malware protection
- Vulnerability management programs
- Security patch deployment policies and processes
- Network access control protection
- Third Party Best Practice tools as typically identified by Gartner Magic Quadrant or other technology rankings such as:
    - Palo Alto Networks
    - Proofpoint TAP
    - Cylance
    - NetWitness
    - Others.

4.3. What tools or practices are effective for integrating the mitigation efforts of third-party service providers with the mitigation efforts of the organization?

- Continuous interaction between the different functions (e.g. Procurement, Cybersecurity) dealing with suppliers/third parties is essential to enhance third party risk mitigation. In order to mitigate the reputational impacts
- Tools providing ready-to-use internal and external communication templates to be used when incidents occur
- Understanding the impacts early on such as impacts to integrity, availability and confidentiality of firm data.
- Assessing the connectivity that exists between the affected vendor and firm, auditing any emails or transactions since detection of the breach.
- Obtaining the Indicators of Compromise and initial infection vector to prevent lateral movement or similar instances from occurring.
- Maintaining a portal of all firm vendors and the services they provide.
    - Each vendor is assigned a Vendor Relationship Officer who serves as their main point of contact at the firm. As part of the incident response efforts, the VRO often will run point and facilitate discussions between the firm and the Vendor. The firm has documentation in place to support the VRO in this work.
- Maintaining Master Service agreements and other contractual documents with the third-party include security incident escalation and coordination language.
- Communication and coordination during a cyber incident occurs with both parties on a common communication platform (audio bridge, Web Conference) to ensure that each party is aware and approves of any actions being taken.
- Business Continuity and Disaster Recovery Testing programs focused on testing with external service providers to provide verification of recovery capability and functional availability during testing scenarios
    - Testing scenarios include:
        - External service provider technology outage
        - Own technology outage
- Initial onboarding and periodic review of 3rd parties using the Information Security and Service Risk Assessments.
- Ensuring contractual assurances that the 3rd party will inform JHI of any security incident affecting JHI systems or data.
- Forensic retainer services

4.4. What additional tools could be useful for including in the component Mitigation?

- Prevention tools should be improved as much as possible, because once the incident occurs, all necessary measures must be activated for incident management: Detect, Protect, Identify, Respond and Recover. Once the situation is resolved, a Post-Incident Analysis is required

- Cyber "immune response" tools which "self-heal" an environment that has been attacked by an adversary such as KineticFuse and other like tools.

4.5. Are there situations in which effective practices for mitigation and restoration activities of the organization are the same or overlap substantially? If yes, please provide examples.

- BCP activities can overlap with cyber mitigation activities as by moving application or processes over to a backup environment may help mitigate the spread of an incident at the same time as restoring the company's ability to continue its business as usual processes.
- Situations when an IT fault or incident occurs that does not appear cyber related where security teams engaged in heightened monitoring and review. This is done to ensure that there are no other attack vectors that are being exploited behind the main attack that could be compromised. In these situations, cybersecurity teams work cooperatively with IT Major Incident Management Team and other Technology teams in parallel on a shared communication platform to coordinate efforts and share appropriate information as the event unfolds or is being mitigated
- If the prior configuration was the weakness that led to the issue. In this case restoration would likely include mitigation.
- IT Change Control processes may require a rollback to a previous release or configuration to mitigate a cyber issue.

5. Restoration

5.1. What tools and processes does your organization have available for restoration?

- List processes in CIRT Runbook required to ensure key tasks are completed before an incident can be formally closed
    - These include return systems to normal operations (recovery and assurance and data restoration)
- Playbooks that include fix forward, restoration of snapshots, backups i.e. layered restoration
- Automated application re-deployment capabilities
- Sheltered Harbor-like capabilities for secure data vaulting
- Disc-based storage solution programs specifically designed to protect backups against data destruction attacks
- Scheduled Backups
- BCP Plans and Testing
- Data Recover and Restore Backups
- Close network vectors of ex-filtration
- Segment critical data to more restricted areas
- Auditing for critical data access
- Industry standard best practice tools and systems to allow for log retention, system and configuration backup/restore, and build processes that will enable the enterprise to recover from an incident
- Tools which may be needed to back out a patch or application update e.g., Tanium and other like products

5.2. Which tools, plans, practices and metrics does your organization use to prioritize restoration activities?

- Risk Level Matrices for classifying security incidents and events implemented throughout the firm. A sample Risk Level (RL) matrix is shown below.

Risk Level (RL)	Condition and Operational impact	Examples
RL1 (High) • Risk deemed unacceptable by Management • The Firm is no longer able to provide some critical services to user(s). • Material loss of Confidentiality, Integrity, Availability • Impact on multiple institutional clients or at least X individual customers • Incident involved unauthorized access to the internal Network by a malicious actor	• Fraud resulting in material loss or major impact to Firm Assets • Regulatory impact likely to result in a finding, enforcement action, or other penalty	• Attack/scan that degrades business critical systems • Earnings release published outside of the firm before proper firm announcement • A host compromised successfully and led to successful lateral movement in the network • Malware that has established communications outside of the firm • High Value Customer/ Low volume of transactions • High volume of transactions / varying customers • A mandatory notification to an EU Information Commissioner's Office required under GDPR
RL2 (Medium) • Known or medium risk with a potential business impact • Partial loss of Confidentiality, Integrity, Availability	• Integrity loss (Sensitive or proprietary information was changed or deleted) • Availability loss (ability to provide a critical service to a subset of system users in or across business functions. • Sensitive data leaves the firm. (e.g.: Client A positions sent to Client B;	• Fraud ring successfully moves money with significant losses • User clicks on phishing email and successfully gave away login credentials or personal information • Unauthorized/ unapproved printed or emailed materials of Network diagrams, Application or Infrastructure architecture has left the firm • Unauthorized production access (lateral movement); Unauthorized device accessing GS Platforms; Unauthorized use of administrator credentials • Firm credential exposure externally • Web site defacement • A mandatory notification to a U.S. or other national regulator
RL3 (Low) • Low risk / Low impact • Firm can still provide all critical services to users but may have lost efficiency. • Minimal loss of Confidentiality, Integrity, Availability	• No sensitive information was exfiltrated, changed, deleted, or otherwise compromised • Control operated as expected	• Employee emails non-sensitive business data to non-approved location • Use of new vendor without proper assessment from vendor risk management team • Privacy incident with no impact/obligation to notify customers or regulators • Identification of a missing/degraded control - may escalate to higher risk level • Credential stuffing attack against any external facing application login page • A voluntary notification to a U.S. or other national regulator
None • Low risk / No business impact • No loss of Confidentiality, Integrity, Availability	• **No business impact** • Control operated as expected • Policy Violation with no business impact	• Employee emails non-sensitive business data to non-existent (not active) account • Unsuccessful attack against an application or infrastructure. • Phishing attack successfully prevented at the perimeter or at the end point. • Misdirected email (internal or external) that is recovered or deleted with no business impact

- Each designation comes with conditions and operational impacts as well as examples. Prioritization is performed by the business based on criticality and risk.
- Business and IT processes are identified, key resources aligned, and overall impact assessment across operational, financial, and resources are defined
- Approved Recovery Strategies that Business Units must use, as appropriate, including Transference or Relocation options to mitigate the impacts of a business continuity event
    - Recovery strategies selected must be consistent with the outcome of Business Continuity Risk Assessments and Business Impact Assessments (BIAs)
    - BC Plans must include appropriate Recovery Strategies that can address a range of impacts of varying severity and duration
    - Business Impact Analysis for all Application and Services to prioritize the restoration activates
    - Some firms use an asset criticality calculator within ServiceNow for all CI's. This can influence the sequence by which services are restored. Standard industry metrics like RTO and RPO are used to measure effectiveness and efficiency of restoration processes.
- NIST-based Security reporting tools are also available that calculates time taken in each and every step during the incident.

5.3. How does your organization minimize undesirable outcomes of restoration activities, such as restoring affected data?

- Financial firms conduct business specific senior leadership exercises through identifying and testing divisional capabilities, and participation in appropriate external exercises with financial sector, industry, and government organizations. Additionally, firms maintain controls that require application deployments to demonstrate the ability to achieve its recorded Recovery Time Objective. In addition:
    - Systems, applications, and data recovery is tested at least annually
    - Firms conduct regular testing data backup and restoral procedures including bare metal restores to verify they are accessible and readable
    - Critical online systems and processes are tested to withstand stresses for extended periods
    - Robust Change Control Processes have been implemented

- Financial firms have developed Incident Response Playbooks and Containment/Isolation Plans
- Firms have implemented Test/Acceptance Environments
- Firms implement system and network segmentation and redundancy
- Firms also maintain geographic diversity of all critical assets (e.g., people, processes, technologies).

6. Improvement

6.1. What are the most effective types of exercises, drills and tests? Why are they considered effective?

- Many financial firms have found that tabletop drills and emergency notification drills to be the most effective types of exercises.
  - Tabletop drills allow the incident response team to engage a diverse cross section of participants ranging from senior level decision makers, legal, compliance, and technology. They are a helpful tool for conveying the importance of having up to date incident response documentation as well as business continuity plans for technology and people. Tabletop exercises are very effective means for testing, learning, knowledge sharing and preparation. Tabletop Exercises also help Cyber, IT and BCP teams walk through potential cyber security incidents, which will give the teams familiarity with the events, and can help identify any potential weaknesses within their recovery plans
  - Emergency notification drills are also valuable, especially when the regular tabletop participants have been through several drills. An Emergency notification drill is when the incident manager (may also be referred to as the incident commander) sends an alert to convene a group of subject matter experts. This "alert" may be in the form of an email, call, or text. The subject matter expert(s) need to respond as quickly as possible. Once they acknowledge the "alert", hey participate in a brief incident management protocol run-through.
- Industry-wide recovery exercises such as the Quantum Dawn series, provide an effective way to evaluate recoverability in the event of a wide scale cyber outage
  - Financial sector exercises that also cross over into power/telecommunications and other critical infrastructures have significant benefit to refining response operations on industries with critical dependencies
- BCP Testing – Ensures application and processes have been correctly assessed and that restored and testing of these applications and processes can meet the company's RTO
  - BCP tests also include incident response, alternate workspace, work from home technologies and communications processes typically take multiple times per year for a firm's most critical processes.
- Red/Purple Team / Penetration Testing Exercises – Firms continually conduct tabletop exercises with business partners in a variety of formats. These are to ensure that a playbook and response acumen are at their peak, should the real-life scenario play out. This will also give us a chance to refine and mature playbooks, if necessary.
- Cyber Incident Response Playbook walkthrough & review – agreed upon procedures to follow during a cyber incident response scenario. This is to ensure information disseminated and actions are taken in the appropriate manner and sequence that we feel are in the best interests of the firm. Playbooks are reviewed continually to ensure its current, especially aligning with any new regulatory policies and/or internal policies.
- Lessons learned from cyber incidents are an important type of "drill" as they are used to improve an institution's risk mitigation capabilities and incident response plans.

6.2. What are the major impediments to establishing cross-sectoral and cross-border exercises?

- The fragmented regulatory landscape, and the lack of a cooperative approach to cyber defense.

- Major impediments are typically variations in cyber lexicon, different regulatory regimes and structures, distinctions in critical functions across sectors and potentially, a lack of understanding of the interdependencies among them that could create ambiguity of impacts.
- Time of day for the exercise is also a significant impediment to cross-border exercises with geographically dispersed support and business organizations. Regional exercises are conducted, where possible, to mitigate these additional issues:
    - Sharing of sensitive crisis management and response protocols
    - Sharing of sensitive information and data
    - Availability of major industry participants
    - Reputational risk / exposure
    - Common taxonomies and misaligned priorities
    - Different regulatory requirements for reporting incidents and their impact. Examples: GDPR, NYDFS, CCPA.

6.3. Which technological aids and tools does your organization consider most useful to improve cyber incident response and recovery?

- There is no "silver bullet"; improvements are a combination of many factors such as:
    - Harmonization of Incident Reporting regulations would make reporting incidents to authorities more effective and less costly
    - 24/7 SOCs and Cyber Fusion Centers
    - 3rd Party Incident Response Retainers
    - FS-ISAC shared Threat Intel.
    - Third Party Threat Intelligence.
    - Forensic Tools
    - Anti-Malware Solutions
    - Case Management and Incident Tracking Tools
    - Automated tools to reduce dependencies on human judgement
    - SIEM and log analysis that leveraged data analytics is a strong resource in quickly identifying incident exposure and building a course of remediation.
    - Strong monitoring systems for each ingress/egress point allow for robust traffic monitoring that can be enhanced with pattern and heuristic alerting of anomalous activity.
    - Various tools such as:
        - Anomali
        - Cylance
        - Flashpoint
        - Netwitness
        - Palo Alto Networks
        - Proofpoint
        - ServiceNow
        - Many others…

7. Coordination and communication

7.1. Does your organization distinguish "coordination activities" from broader "communication" in general? If yes, please describe the distinct nature of each component.

- Communication refers to the ability of an organization to mobilize and engage the appropriate resources that are needed to work an incident. This also is the mechanism that would inform senior leaders and other stakeholders of periodic status, impact, mitigation activities, and resolution. External communication activities are the responsibility of a Corporate Communications team with those outside of the internal

stakeholder circle that are impacted by the cyber incident. All communications internally or externally follow the agreed communications plans and must be agreed by the Crisis Management Team.

- Coordination are the sets of activities, processes, roles & responsibilities, and systems that enable various cyber security and IT professionals to work collaboratively to determine the source of the fault, take action to mitigate the impact, and ultimately resolve the issue. Coordination activities refer to internal activities to ensure all internal stakeholders are plugged into the incident and are providing their inputs, per a playbook.
- Cybersecurity Fusion Centers are charged with assessing, detecting, and responding to Cyber Events that threaten the Firm's clients, assets, and reputation
    - Fusion is also the focal point for cyber coordination, communications and reporting, to include with leadership, as well as with external parties (e.g., peers, media, regulators, law enforcement)

7.2. How does your organization address the possibility that email or traditional communication channels will be unavailable during a cyber incident?

- Organizations have established redundant communication methods that would be leveraged in the event of loss of primary or traditional communication methods. These include both audio and video capabilities that are externally hosted and use of private secure government networks such as the DHS Government Emergency Telecommunications Service (GETS).
- Use of RNS via phone/text/email
- Use of offline cloud-based email systems invoked during incident
- Approved Out of Band communication methods are agreed by the Incident Response teams and wider Crisis Management Teams.
- Phone based incident/information alerting tools.
- Alternative communication/collaboration channels.
- Texting and/or mobile phone calls, where possible and as needed.
- Use of Emergency Notification Systems (e.g., Everbridge, MIR3 et al)

7.3. Apart from regulatory/compliance reporting, what other information does your organization consider useful to share with authorities?

- Financial firms find it useful to share information about their cybersecurity programs, including opportunities Firms some challenges, with authorities to inform their view of policy and/or regulation in this emerging space. firm also finds it valuable to exchange cybersecurity information and collaborate with law enforcement and other non-regulatory government entities on initiatives that make us collectively better at addressing cyber threats, such as:
    - Attack methods and threat intelligence can be useful for authorities, with consideration given to the protected or sensitive information
    - High level overview of the main countermeasures activated
    - Consultations on various upcoming regulations/papers
    - When appropriate, sharing advance insights on threats to our industry or sector that we obtain through our Threat Intelligence processes with authorities
    - Emerging cyber threats which we predict with a medium to high level of confidence
    - Specific, detailed and technical information regarding the incident are shared only with competent authorities, according to the regulatory requirements in force or when expressively required
    - Information on ongoing threats/incidents is already being shared with authorities and key stakeholders from a collaboration perspective (e.g. CERTFin, FIRST, FS-ISAC, etc.)

Other Comments

- Part 2 Preparation: Financial firms would like to recommend that FSB maintain a compendium of all applicable cyber regulatory requirements. This would be beneficial for organizations with a global presence to understand all rules, regulations and guidance in force.
- Item 18: Financial firms would like to suggest, that aside from designating a primary and alternate 3rd party cybersecurity provider, multi-layered defense controls could also be put in place. Such controls may be able to provide overall resilience addressing individual 3rd party cybersecurity provider issues.
- Item 19: Financial firms would like to propose that the defined taxonomy should be flexible and agile enough such that it can be easily used for defining and classifying the incident based on the different requirements/contexts/business environments across jurisdictions. While organizations can and should have a pre-defined and consistent classification method, they should also be prepared to easily transform based on current datasets, to be able to derive different classifications based on unique requirements in different locations.
- Item 21: Financial firms would like to respectfully suggest that FSB encourage financial authorities to leverage existing intel/incident sharing forums instead of creating new ones in each of the jurisdictions. Cross-border and cross-sectoral sharing bring more intel/information than jurisdiction-siloed fora.
- Item 35: Financial firms would like to recommend that financial authorities define the maturity level of the cyber incident reporting requirements (CIRR criteria, reporting processes) to align with regulatory requirements on cyber resilience and corresponding maturity levels.
- Item 43: Financial firms appreciate FSB's recognition of the need to do cross-border coordination as norm if not a necessity in the globalized environment that we operate in. We continue to support cross border-data transfers required in cross-border coordination activities to harness the strength of the digital economy. By doing so, financial firms are able to utilize efficiencies and as well as the competitive advantages that global organizations bring.
- Item 46: Financial firms advocate for regulatory consistency and respectfully propose that financial authorities harmonize cyber incident reporting requirements (criteria, reporting processes), and cyber readiness exercise expectations (tabletops, drills, etc.). Coherence across jurisdictions will streamline organizational processes, making them more effective, enabling them to focus on responding to and recovering from the incidents as well improving the resiliency posture.
- General Suggestion: Financial firms would like to recommend that FSB consider including effective CIRR practices applicable when majority of the personnel are working from home/away from office.
- General Suggestion: Financial firms would like to suggest that FSB/industry encourage financial authorities to leverage their existing recovery frameworks (including business continuity/crisis management processes) as part of the cyber incident recovery phase to help ensure appropriate stakeholder participation and raise preparedness levels to combat emerging cyber threats.