INSTITUTE of INTERNATIONAL FINANCE

June 2021

Effective Cyber Incident Reporting: a call for greater consistency, improved information-sharing and closer cross-border cooperation

Martin Boer, Director, Regulatory Affairs (mboer@iif.com)
Melanie Idler, Senior Policy Associate, Regulatory Affairs (midler@iif.com)[1]

Overview

Financial firms are uniquely positioned to play an important role in supporting and protecting the overall cyber resilience of the financial system. Whenever a financial firm identifies a cyber security incident that rises to a financial institution's predefined threshold of materiality, it is legally required to disclose it to the relevant authorities. Cyber incident reporting can be a beneficial tool that helps protect the overall financial system by making authorities aware of specific incidents and alerting them to issues that could be impacting other parts of the financial system, including in other jurisdictions. Depending on how authorities respond to the information, it can also help firms recover faster and prevent other organizations from being impacted by that same (or similar) cyber incident. In practice, however, cyber incident reporting is less effective than it can be due to ambiguity around how firms and authorities define what constitutes a *cyber incident*, and differing approaches and reporting requirements across the various authorities. These differences are compounded by insufficient information-sharing, including from authorities *to* firms, and inadequate cross-border cooperation and collaboration.

This IIF Paper sets out to explain the current approach to cyber incident reporting across key jurisdictions and the ways in which it can be improved. Ambiguity around definitions has created regulatory fragmentation across firms and authorities. The substantial differences between stakeholders in terms of what information needs to be shared about cyber incidents, within what timeframe, and even the format in which the information needs to be submitted, may lead to inconsistencies across jurisdictions that can limit the effectiveness of information shared by authorities to financial firms regarding the threat landscape, and potentially impeding similarly affected or vulnerable firms from addressing the cyber incident quickly and effectively. To help address these issues this paper also suggests several industry practices, as well as policy

[1] Special thanks to Mary Frances Monroe and Katharina Sobczak for their contributions to this paper.

recommendations to help promote greater consistency and closer cooperation to support effective cyber incident reporting, within and across borders.

Introduction

Cyber incidents can be either *intentional*, where malicious adversaries are targeting organizations on purpose or *accidental*, where something goes wrong, such as when upgrading an IT system or using a new piece of software or hardware. The Bank for International Settlements estimates that approximately 40% of cyber incidents are intentional and malicious, rather than accidental.[2] In the case of intentional cyber incidents, the financial services industry has long been targeted by malicious cyber actors due to the potential for financial gain from access to confidential financial data. In 2020, the average cost of a data breach to financial institutions was USD 5.9 million,[3] and it is estimated that average annual losses due to cyberattacks in the financial industry are between USD 38 billion to 100 billion per year.[4] Given the enormous costs at stake, both financial and reputational, whenever a cyber incident is discovered by a financial institution, it is quick to address the threat within the organization. However, even if one firm manages to discover and contain a breach, the adversary is often simultaneously targeting other firms, crossing borders, and taking advantage of the global reach and scalability of the internet, as well as the interconnectedness of the financial ecosystem. Furthermore, with each breach, threat actors gain a better understanding of the networks and operations of financial institutions, enabling them to launch even more disruptive or destructive attacks in the future (or sell such knowledge and capabilities to others). Conversely, when cyber incidents are accidental, which may occur with the introduction, upgrading, or modification of IT systems, hardware, and software, there is less urgency around reporting, so long as the accidental incident does not rise to the level of a material incident. Nonetheless, it is important for the details of such cases to be shared quickly to prevent other organizations from experiencing similar cyber incidents.

Given the increasing number, and growing cost and severity of cyber incidents, including recent high-profile breaches affecting SolarWinds and Microsoft Exchange, there should be a common interest among all firms – and the authorities – for the information related to the cyber incident to be shared quickly and efficiently. This could help prevent incidents from reaching other parts of the financial system and spreading across the entire digital economy, and possibly undermining financial stability. Indeed, effective cyber incident reporting has become a critical part of a comprehensive cyber risk management framework. Financial institutions have long been required to report operational disruptions to the relevant supervisory authorities as part of their regulatory obligations. In the past decade, as the frequency and severity of cyber incidents have increased, it became increasingly apparent that more guidance and rulemaking would be needed to assist financial institutions. Supervisory authorities moved to expand operational risk reporting frameworks to include the reporting of cyber-related incidents that were material or had the potential to help other financial institutions adapt their cybersecurity practices and procedures to the evolving threat landscape.

Since then, several cyber incident reporting frameworks have been introduced by regulators and standard-setting bodies worldwide. The information that is collected is intended to help firms and supervisors alike understand the causes and impacts of different operational events affecting

[2] BIS Working Papers, "The drivers of cyber risk", May 2020.
[3] IBM Security, "Cost of a Data Breach Report 2020," July 29, 2020.
[4] Risk.net, "Cyber modelling masks scale of potential losses, study finds," March 27, 2019.

institutions, identify common events, develop new rulemaking or guidance that may be used to lower the frequency and/or impact of operational events, and inform financial institutions of common threats and impacts. However, the lack of coordination among regulators has resulted in fragmented reporting requirements that may require the firm to provide authorities with completely different data sets and/or granularity of information.[5]

The definition of an incident and its level of impact to the firm's operations form the foundation of a supervisory incident reporting framework, yet disparities between terms have led to diverging decisions about which incidents are reportable to authorities. Current incident reporting frameworks have significant differences in the definition of the terms *cyber incident* and *cyber event*, and they are often used interchangeably, which creates an additional layer of complexity. Further, materiality bifurcates these incidents that supervisors may deem "of interest" for reporting. Depending on the authority and their remit (e.g., financial stability, consumer safety), materiality thresholds may change or focus on different data elements, increasing the complexity of information that firms must collect to fulfil their reporting obligations. It is important for financial institutions to be able to determine their own materiality thresholds because they know their own risks and their own risk tolerance, but regulators should hold industry to certain standards when it comes to firm viability and overall financial stability.

This disparate jurisdictional reporting framework is at odds with the interconnected and borderless networks operating worldwide. Cyber threats and growing digitalization are increasing systemic risk to the infrastructure of financial markets, and the broader digital economy. Incident reporting has the potential to inform the financial industry of imminent threats, or drive awareness of more medium- or long-term changes to the threat landscape. For incident reporting to have a meaningful impact on threat mitigation, it is imperative to have a mechanism for the multidirectional sharing of information between firms, firms and authorities, and between the authorities themselves. This information sharing should also allow for the rapid identification of threats across multiple firms or across multiple financial sectors. For medium- and long-term threat landscape changes, the ability for firms to provide uniform reporting enhances the authorities' ability to gain and report insights from firm incident reporting which, in turn, could raise the floor of the financial industry's preparedness against these threats.

The growing frequency and unprecedented scale of recent cyberattacks should engender newfound momentum and increased interest among all firms – and the authorities – to create a repository where information on cyber incidents can be shared quickly and effectively to prevent attacks from impacting other parts of the financial system and the larger digital economy. While regulation can be an important tool for bolstering cyber resilience, there are times when it can also inadvertently increase cyber-risk if the approaches are conflicting and resource-draining, or if firms face several differing jurisdictional standards and practices. By contrast, globally accepted standards, industry best practices, and consistent implementation can significantly enhance cyber resilience by creating streamlined, meaningful, informative, and non-duplicative reporting that enhances the understanding of the threat landscape faced by the financial service industry and allows for strong correlation of cyber or operational activity between different types of financial institutions.

[5] In a 2017 global review of mandatory cyber incident disclosure requirements, the Financial Stability Board (FSB) found 56 different schemes of regulations and guidance for cybersecurity across the 25 FSB member jurisdictions, of which most of the elements include regulatory reporting (50) and information sharing (31).

Dueling Definitions and Terms Classification

Categorization is an important step in developing the underlying cyber incident reporting framework and provides the basis for analysis and reporting. One of the primary challenges for supervisors is their ability to gather sufficient information from financial institutions to understand which events or incidents are, in fact, material and important. Supervisory incident reporting frameworks use the terms, *cyber incident* and *cyber event*, to define the universe of potentially reportable events. Separately, these frameworks define materiality as a means to focus firm reporting to cyber incidents that are of particular interest to the authority.

When viewed across multiple authorities, the terms *cyber incident* and *cyber event* are often used interchangeably. The Computer Security Resource Center at the U.S. National Institute of Standards and Technology (U.S. NIST) defines "computer security incident" as follows, and refers readers to cyber incidents and events:

> *An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security procedures or acceptable use policies.*[6]

Existing definitions of cyber incidents, through the inclusion of words such as 'potential', 'imminent', and 'jeopardize', may introduce thousands or millions of cyber events per day where there was no actual loss of data confidentiality, integrity, or availability nor any business impact. Other terminology created for the industry (see Text Box I for examples of widely used definitions) can be tailored to the needs of individual firms operating across different jurisdictions and industries, while reporting to various regulators.

For the sake of discussion, we will define a *cyber incident* as:

> *The occurrence of actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.*

Whereas a *cyber event* is defined as:

> *The occurrence of actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security procedures or acceptable use policies.*

When defined in this manner, cyber incidents are a subset of cyber events. Materiality and intent have been left out of these definitions as neither the size of the occurrence nor the executor's intent determines whether an incident or an event has occurred. When firms start to review these occurrences using this new definition of cyber incident, the universe for potential reporting is substantially decreased. Firms are best situated to assess the level of impact (materiality) that is created by the cyber incident and to determine if reporting requirements are triggered.

[6] NIST SP 800-128 under incident from 44 USC 3552.

Once a financial institution classifies an event as a cyber incident that meets the materiality threshold, it should be escalated and reported to relevant stakeholders within the firm, up to and including the Board, as well as different authorities and regulators and, depending on the firm's contractual obligations, its customers, and clients. Typically, the cyber security incident report includes the nature of the incident, measures taken following the incident, and remediation to avoid recurrence. The financial firm's decision to escalate and report depends on the severity of the incident, the contractual relationship, and legal and regulatory obligations.

Establishing standard industry terminology for cyber incident reporting that improves the quality of information shared, generates greater analysis and understanding and enhances communication between stakeholders, would be beneficial across the private and public sectors.

Jurisdictional Reporting Requirements

For financial firms operating across different countries, the rules and regulations around cyber security incident reporting can also differ substantially. Firms are subject to various incident reporting and notification requirements and different reporting timelines in jurisdictions around the world. If the incident involves data, especially consumer data, it becomes even more complex and can involve customer data protection standards, some of which include material penalties for data breaches.

In 2018, the Financial Stability Board (FSB) released the *Cybersecurity Lexicon*, which was intended to promote a cross- sectoral, common understanding of relevant cybersecurity terminology across the financial industry, including among authorities and other industries.[7] While the FSB Lexicon was a necessary first step towards reducing regulatory fragmentation and promoting a common understanding of cyber security terminology, its definition of a cyber incident is not entirely consistent with the US NIST, NY Department of Financial Services (NYDFS) and the EU Network and Information Security directive (EU NIS Directive) concepts of who the perpetrator is (malicious vs. accidental), whether the incident is a "successful" breach or not ("jeopardizes" vs. actual) and whether any harm was done.

TEXT BOX I: DEFINING A "CYBER INCIDENT"

U.S. NIST defines an "incident" as: *An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.*

NYDFS applies a definition of a "cyber event" that means: *any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.*

The FSB CYBER LEXICON defines "cyber incident" by adapting the NIST definition as: *A cyber event that jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.*

The EU NIS DIRECTIVE defines a "cyber incident" as: *An 'incident' means any event having an actual adverse effect on the security of network and information systems.*

In the recently published FSB toolkit on effective practices for cyber incident response and recovery (CIRR),[8] the FSB considers reviewing the FSB Lexicon and enhancing the coordination

[7] Financial Stability Board, "Cyber Lexicon," Nov. 12, 2018.
[8] Financial Stability Board "Effective Practices for Cyber Incident Response and Recovery" Oct. 19, 2020.

as a part of its work program. In its draft toolkit consultation, the FSB explicitly highlighted 'significant' incidents as in scope as reportable incidents. Yet in its final report, the FSB emphasized deference to national authorities' reporting requirements.

Although some firms purport to follow the wide-reaching terminology set out by the NIST, NYS DFS, FSB Cyber Lexicon, NIS Directive, or other regional bodies, given the speed of developments around cyber resilience, and the lack of a harmonized industry definition as to what constitutes a cyber incident, firms often use their own definitions, created for their specific business needs rather than only following existing international definitions and standards. Taken together, these diverging approaches are unlikely to mitigate, and may actually increase regulatory and market fragmentation across various jurisdictions going forward.

Regulatory mandated timeframes for incident and notification reporting also vary. In January 2021, the Federal Reserve, Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) issued a proposed rule that would require banks to notify their regulator of a "computer security incident" "as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred."[9] If adopted, this 36-hour notification timeframe would supersede the NYDFS Cybersecurity Regulation (2017), which had established that organizations must submit notification of a data breach within 72-hours of discovery. Meanwhile, the ECB requires supervised entities to report cyber incidents within two hours of their initial detection. The proposed rule is intended to enforce immediate communication between regulators and their supervised institutions in the event of a cyber incident that limits customer communications or services. It will also require service providers to notify the banks they work with if they experience a cyber security breach.

While the proposed US agency rule focuses on notification, not reporting, it is reasonable for firms to expect follow-up requests for further incident details that may culminate in an incident report. This is especially the case if firms lack detailed information to provide to regulators during the initial 36-hour notification timeframe.

Overall, the differences in jurisdictional regulatory approaches can be viewed in the following ways:

- Challenges in reporting a single incident to multiple authorities and complying with different thresholds and inconsistent definitions and/or thresholds of materiality, types of data sets, communication channels, perspectives (e.g., payment, critical infrastructure);
- Different taxonomies for how to notify the various regulatory authorities;
- Differences in what types and/or nature of a cyber incident are in scope;[10]
- Deadlines for reporting cyber incidents differ from country to country, with regulators requiring firms to notify "as soon as possible" and "without undue delay," and, depending on the regulatory authority, within two, 24, 36, or 72 hours; and,
- Multiple stakeholders involved in an incident reporting process.

[9] Federal Register, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" Jan. 2021.
[10] Financial Times "US banks face tighter scrutiny of cyber defences" June 16, 2019.

The recent Digital Finance Package adopted by the European Commission includes proposals for a new Europe-wide Digital Operational Resilience Act (DORA)[11] that would mandate harmonized incident reporting across Europe's Member States:

> *Harmonising and streamlining the reporting of [information and communication technology] ICT-related incidents is achieved via, first, a general requirement for financial entities to establish and implement a management process to monitor and log ICT-related incidents, followed by an obligation to classify them based on criteria detailed in the regulation and further developed by the ESAs through to specify materiality thresholds. Second, only ICT-related incidents that are deemed major must be reported to the competent authorities. The reporting should be processed using a common template and following a harmonised procedure as developed by the [European Supervisory Authorities] ESAs.*

Going forward, a globally coordinated framework for reportable incident notification, establishing common definitions and terminology, as well as clear communication amongst stakeholders, can help to ensure a common understanding of relevant reporting obligations and improve consistency between otherwise overlapping guidance.

Response Plans in Practice

Incident response plans are typically required by supervisory authorities. A key part of managing an incident successfully is having a robust and effective prevention and cyber incident response framework in place that is regularly tested, efficiently reported, and includes scenario analysis, plans, and playbooks. Once a cybersecurity incident occurs, a financial institution is expected to fulfill mandatory incident reporting requirements and execute its incident response plan.[12]

With respect to the current COVID-19 pandemic, firms and authorities have had to adjust their cyber risk management processes and cyber incident response and recovery activities as part of their transition to remote work and operations. Participation in 'preparatory activities,' such as simulation training, can help mitigate threats and help identify vulnerabilities at the perimeter of critical networks, thereby reducing the overall likelihood of an incident occurring.

A robust and effective prevention and cyber incident response plan, as defined by ISO standard 27035,[13] establishes five key categories:

1. Prepare: Establish a Cyber Incident Response Team structure and have an incident management plan in place.
2. Identify: Thresholds and procedures to activate the incident response: understanding the type and the severity of an incident.
3. Assess: Categorization of an incident and escalation, including decision making process.
4. Respond: Procedures for the containment of the impact of cybersecurity incidents, the activation of the recovery process.
5. Lessons Learned: Prioritization of relevant learning points and remediation activity to effectively mitigate and remove any identified vulnerabilities.

[11] European Union "Digital Operational Resilience Act" Sep. 24, 2020.
[12] See for example Monetary Authority of Singapore "Instructions on Incident Notification and Reporting to MAS" June 21, 2013.
[13] International Organization for Standardization "ISO 27035" Nov. 2016.

Large international firms have the staff and resources to manage cybersecurity operations in-house. However, less mature firms sometimes outsource these operations to third-party service providers, which can create an additional notification layer between event analysis and reporting by the firm that may make real-time reporting more challenging, or in some cases, infeasible. Financial institutions may also choose to communicate the minimum information required until a full investigation can be completed. Some regulators, however, require the completion of an additional supervisory review of post-incident learning. In some cases, firms are asked for multiple updates of a post-incident assessment after an incident is initially reported. While there are benefits to "lessons learned" post-incident exercises, the lack of feedback from regulators, and the inconsistent guidance around additional post-incident notifications, may create additional, unnecessary layers of complexity.

Having the right cybersecurity incident management program in place is essential, as it allows firms to turn their attention to the incidents that are material in a timely fashion. Finally, close cooperation as well as a clear division of tasks between technical teams dealing with technical incident management, on the one hand, and regulators dealing with the potential systemic or financial stability consequences of the incident, on the other hand, are critical.

Proposed Policy Measures and Industry Practices

Timely response to detected cyber incidents is crucial to support cyber resilience across the financial system. Given the global and constantly evolving nature of cyber incidents, coordination on existing standards and frameworks that align with international best practices is critical.[14]

The financial services industry would benefit from greater consistency across policy measures based on common industry practices. These should be principles- and risk-based and proportionate, while considering the different risk profiles, cyber maturity, and business models of respective firms.

The diversity of reporting requirements and standards can undermine the efficiency and effectiveness of reporting for firms. Further, the diversity of information reported to authorities limits the ability of authorities to synthesize the information reported by firms, and ultimately could dilute the value of this reporting to the authorities, as well as the information that could be further shared to the firms to prepare the financial industry for material operational events or changes in the threat landscape. That includes resources that could be dedicated to resolving the cyber incident. A more consistent approach to incident reporting, seeking similar outcomes, could help reduce the number of similar, but not identical, industry cyber incident reporting requirements.

By making reporting conventions more consistent internationally and minimizing discrepancies in expectations across frameworks in different countries, regulators can ensure that cyber incidents are reported quickly and effectively in a manner that delivers the outcomes expected

[14] Two international standards preferred by cross-border organizations are: NIST's Framework for Improving Critical Infrastructure Cybersecurity and CPMI-IOSCO's Guidance on Cyber Resilience for Financial Market Infrastructure.

by supervisors and financial institutions alike. This could be achieved by focusing on the following seven areas:

1. Standardization of key terminology;
2. Standardization of reporting timeframes and incident reporting templates across jurisdictions;
3. Creation of a common taxonomy for regulatory notification of cyber incidents;
4. Closer cooperation through industry information-sharing platforms;
5. Enhanced cross-border architecture for information sharing;
6. Greater information sharing from regulators to supervised financial institutions; and,
7. Ensuring that policy measures are risk-based and outcome-based, and support innovation.

1. Standardization of key terminology

As detailed above, the definition of a *cyber incident* differs across standard-setters and jurisdictions. Small divergences in applied terminology may pose a significant impact for firms in practice. Clear and consistent definitions across existing reporting requirements would greatly benefit both authorities and industry to prioritize what should be reported, enabling efficient allocation of resources, higher quality analysis, and ultimately improving real-time collaboration between firms and regulators. At the same time, the definition of a cyber incident should be flexible enough to remain relevant over time by avoiding references to technical specifications (e.g., specific IT language, platforms and/ or technology) or defining a common set of information to be collected for each incident. Furthermore, it is important to define the scope of reportable cyber incidents (e.g., materiality), and clarify the objectives of the reported incidents and the incident type in terms of its replicability or repeatability.

Moreover, it is also important to agree on clearer frameworks around materiality thresholds to prioritize the urgency of reported incidents. Materiality thresholds should be based on impact to a firm's respective operations (e.g., business lines, systems, sensitive information) and market impact to avoid reporting incidents that are insignificant and below the materiality threshold, allowing better proportionality and scaling across a range of institutions, while reporting only incidents that are significant to a material part of the larger organization. Materiality for example could be risk-assessed using several factors, such as disruption or impact to confidentiality, integrity or availability of information assets, and the related potential client or market impacts. A common materiality threshold would reduce reporting burdens and improve data quality. The FSB, already having published the *Cyber Lexicon*, where some definitions relied on those conceived by standards bodies, is well placed to address these issues in future updates to the Lexicon, and member jurisdictions are encouraged to refer in their regulation to the agreed upon FSB definitions.

2. Standardization of incident reporting templates

Harmonizing regulatory and supervisory reporting templates globally would help reduce the regulatory burden on firms and ensure consistency of messaging across all jurisdictions under which a firm may be regulated. During a single cyber incident, firms may need to engage with a broad range of regulatory and law enforcement bodies around the world, which often requires compliance with multiple regulatory information-sharing protocols and incident reporting

templates. A clear, appropriate, and harmonized incident reporting template would bring benefits to both the private and public sectors. Use of a single common incident reporting template could allow firms to report a cyber incident once, rather than reporting a single incident to multiple regulators with different, competing reporting templates and timelines. This would allow the affected firm to focus its resources on addressing the cyber incident internally, instead of filing multiple incident reports with the various regulators. It would also benefit regulators who would receive the information at relatively the same time, and thereby might afford them precious time to prevent similar cyber incidents from occurring.

3. Creation of a common taxonomy for regulatory notification of cyber incidents

Global financial institutions face a significant challenge in terms of variation and a lack of standardized incident reporting across their operating jurisdictions. This is compounded by the use and deployment of globally shared systems and services that operate in, or support, many jurisdictions simultaneously. Taxonomies used today are jurisdiction-specific and do not rely on harmonized concepts and definitions. In the current regulatory environment, firms may take different interpretations as to when an incident is reportable, leaving regulators with potential misinterpretations of the threat landscape. A common taxonomy on which incidents are reported and how could promote consistency and alignment across jurisdictions. This concern can be addressed by creating a common taxonomy for reporting incidents to regulators that can be used globally, and in line with internationally recognized industry standards, including the Guidance on cyber resilience for financial market infrastructures published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) (CPMI-IOSCO Guidance), the US NIST Cybersecurity Framework, and the ISO 27000 Series, which provides information security control standards.

A good example of a widespread taxonomy is the industry-developed *Financial Sector Profile*,[15] a set of over 250 financial-sector specific cyber controls intended to improve uniformity and overall cyber resiliency. Using a financial firm's self-assessment against the Profile eliminates the need for examiners to repeatedly ask basic security questions, providing significant efficiencies for both regulators and financial firms. The Profile was launched by several trade associations, including the IIF, and has also been accepted by many regulators around the world as a means to demonstrate compliance with cyber security regulations.

4. Closer cooperation through industry information-sharing platforms

There is a need for streamlined reporting mechanisms that gather information on an aggregated level and promote best practices in a financial ecosystem that increasingly operates on digital infrastructure. Currently, there are several platforms being used on a largely voluntary basis that increase operational collaboration among banks, including: The Financial Services Information Sharing and Analysis Center (FS-ISAC),[16] and Analysis and Resilience Center (ARC).[17] These platforms collect and provide their members with information on potential vulnerabilities, including actionable warnings of physical, operational, and cyber-threats or attacks on the

[15] IIF "Industry Unveils Cybersecurity Profile to Help Financial Institutions Develop and Maintain Cyber Risk Management Programs" Oct. 25, 2018.
[16] FS-ISAC is an industry consortium dedicated to reducing cyber-risk in the global financial system and hosts FS-ISACs around the world that bring together financial institutions.
[17] Formerly known as the Financial Systemic Analysis and Resilience Center (FSARC).

national financial services infrastructures. Except for three jurisdictions[18] (i.e., Brazil, Japan, and Saudi Arabia) where the cybersecurity information-sharing amongst banks is mandated through regulations or statutes, in most jurisdictions the practice is for supervisors to not be directly involved in these platforms. There are other less documented or systemic types of information-sharing channels in place (i.e., regulator-to-regulator), that occur on ad hoc or bilateral bases, and vary widely across jurisdictions.

Going forward, more could be done globally to improve cyber incident information sharing by exploring ways in which existing information sharing initiatives can provide legal protections from liability and initiatives for participating firms. That would increase efficiency in sharing incident-related intelligence internationally and would further promote best practices on reporting cyber incidents. Greater cooperation, coordination, and exchange of threat information between firms (and authorities) can therefore provide critical, advanced notice of impending threats, and provide crucial time to prepare.

5. Enhanced cross-border architecture for information sharing

It should be easier to implement multidirectional information sharing on cyber incidents between firms, between firms and authorities, and between authorities themselves. Although various initiatives are already in place to facilitate secure and trusted sharing of threat information, authorities can play an important role in harmonizing and coordinating requests for information, possibly including a global, standardized reporting platform, sharing insights and best practices on reported cyber incidents. Greater coordination would introduce greater efficiency and possibly reduce reporting burdens for firms. Policymakers should look to ensure strong cooperation arrangements and relationships with regulators in other major jurisdictions. This is an area where home jurisdictions can play a coordinating role in sharing any relevant information with host jurisdictions.

6. Greater information sharing from regulators to supervised financial institutions

Lack of feedback from regulators to institutions about reported information is a critical issue for many financial firms. Currently, there are relatively few mechanisms in place to receive aggregated information/feedback from regulators. Further, the information provided by firms to authorities under the current, disparate cyber incident reporting frameworks may not lend itself to effectively communicating valuable information back to the financial services industry. Firms would benefit from more clarity on what regulators are seeking in terms of incident reporting to improve the quality of information and consistent data points that may drive the visibility of the authorities to the threat landscape.

It is important that all stakeholders agree on the purpose of the reporting, and which information needs to be shared. The industry would benefit from greater, and more granular, information sharing from regulators back to the firms. While more mature regulators are already sharing anonymized information on cyber incidents and threats with the private sector, thus promoting cyber resilience within the financial industry,[19] other regulators tend to share less. In any new incident reporting framework, policymakers should consider creating more bilateral, two-way

[18] Basel Committee on Banking Supervision "Cyber-resilience: Range of practices" Dec. 2018.
19 European Central Bank "What is cyber resilience?"

sharing of information. Interests are aligned to share critical information quickly to help contain the impact of cyber incidents across the industry and to support the overall cyber resilience and stability of the financial system.

7. Ensuring that policy measures and regulatory requirements are risk-based and outcome-based, and support innovation

Any new regulatory policy should be flexible and outcome-based, allowing firms to employ technological advancements and the most robust practices going forward. As cybersecurity practices and procedures continue to evolve, firms should be encouraged to innovate on prevention, detection, and response solutions, and collaborate to ensure their cyber incident reporting remains effective and relevant. It is important that any framework or guidance is technology-agnostic, encouraging firms to best protect themselves while retaining flexibility for firms to do it in a proportionate manner that is most appropriate for them and relative to their overall cybersecurity maturity. Given the global nature of many cyber incidents, it might in some cases be appropriate for solutions to be managed centrally, at headquarters, rather than separately in each jurisdiction where the firm operates.

Conclusion

Collecting relevant and accurate information on cyber incident reporting, and sharing it with peers and authorities, is crucial to supporting cyber resilience and financial stability across the financial industry. It is important that global standard-setters, including the FSB, encourage and work closely with sectoral standard setters and regional and national authorities to coordinate cyber incident reporting practices, in addition to clarifying definitions and creating a common taxonomy.

Public-private platforms and enhanced information-sharing practices can also support more effective reporting. Any new guidance should be principles and risk-based, and technology-agnostic, allowing for the incorporation of the latest technological opportunities and innovations available. Moreover, it should provide clarity and access to best practices for financial institutions, thereby contributing to more consistent, and ultimately more effective, cyber incident reporting. Regulators should continue to collaborate and develop sector-specific requirements and guidance, reflecting both the needs and capabilities of each part of the financial industry.