ADDRESSING REGULATORY FRAGMENTATION TO SUPPORT A CYBER-RESILIENT GLOBAL FINANCIAL SERVICES INDUSTRY

April 2018

Jaime Vazquez, Policy Advisor, Regulatory Affairs, jvazquez@iif.com
Martin Boer, Director, Regulatory Affairs, mboer@iif.com

Given the continuing development of regulation aimed at strengthening cyber-resilience across the financial services industry, the objective of this paper, produced by the IIF Cybersecurity Working Group, is to evaluate the regulatory approaches being introduced around the world and to identify areas where regulatory fragmentation is occurring. In that vein, the IIF encourages the Financial Stability Board, in collaboration with other authorities, to find ways to design a more consistent and coordinated regulatory landscape going forward.

That landscape should ideally be built around a principles-based and risk-based global framework, similar to the NIST Cybersecurity Framework in the U.S., that would provide a common approach for all the cyber-related areas where public and private incentives are aligned. Where interests are not identically aligned, further regulation might be needed, but it should be developed in coherence with the overall framework and in accordance with leading practices that avoid, to the extent possible, creating fragmentation. That would both effectively enhance the cyber-resilience of the global financial sector and contribute to reducing overall risks to financial stability.

BACKGROUND AND SCOPE:

Cyber incidents can disrupt critical financial services and thereby undermine the security and confidence of the financial system. If the attack is large enough it could even lead to the disruption of the global financial system and on overall financial stability.[1] Therefore the increase in number, scope, and sophistication of cyber-attacks presents an increasing threat to the financial sector. As such, individual financial institutions have been investing heavily in control functions to counter these threats, increasing risk awareness across firms, and safeguarding critical assets and data.

Understandably, authorities around the world have also developed strategic initiatives, guidance papers, regulatory and supervisory approaches (henceforth, Regulations) aimed at strengthening the cyber-resilience of both individual institutions and the global financial system. Note that we refer to the concept of "cyber-resilience" rather than the narrower term of "cybersecurity." The latter refers only to technologies, processes and measures that are designed to protect systems, networks, and data from cyber-attacks and other incidents, whereas cyber-resilience is about maintaining the entity´s overall ability to deliver the intended outcome continuously at all times, even when regular delivery mechanisms have failed, such as during a crisis or when a security breach occurs. Being cyber resilient includes the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

1 See Communiqué G20 Finance Ministers and Central Bank Governors Meeting Baden-Baden, Germany, 17-18 March 2017, Baden Baden. March 2017.

However, the resilience of the financial sector not only depends on its components (including banks, insurers, financial market infrastructure, etc.), but also on other sectors that play critical roles as well, such as energy, telecommunications, and cloud providers, because of their interconnectedness to the financial system's IT and data infrastructure. These types of critical infrastructure are meaningful contributors to the security of national economies. While this paper is focused on the financial sector itself, the failure of any of those critical national infrastructure, from an operational and from a cyber-risk point of view, may be more important than the failure of any individual financial institution.

This paper focuses specifically on regulations for financial institutions, which can cover a wide range of issues, including cyber-strategy, which is about setting the overall approach of the entity regarding cybersecurity; governance, which refers to the establishment of policies and definitions of roles and responsibilities within each organization such that the strategy can be carried forward; data protection in a broad sense; information sharing among banks, with supervisors or other authorities; penetration testing (pen-testing) to test computer systems, networks, or web applications to find vulnerabilities that hackers could exploit; and supervisory approaches to address cyber-risk.

Although regulation can be an important tool in bolstering cyber-resilience, it can also inadvertently increase cyber-risk if regulatory approaches are conflicting, or resource draining, and more so if there is a lack of a unified approach to addressing cyber-risk management for the overall financial services sector. Regulation is needed around the global threat of cyber-risk but too often jurisdictions hold differing views on how to address these risks. A 2017 Financial Stability Institute policy paper highlights that for some regulators "...cyber-risk is not amenable to specific regulation and that cyber-issues can be handled with existing regulation relating to technology and/or operational risk" while in other jurisdictions regulation is formed around the notion that "...regulatory structure is needed to deal with the unique nature of cyber-risk, and given the growing threats resulting from an increasingly digitized financial sector."[2]

In any case, and as jurisdictions continue to develop new regulatory approaches to cybersecurity, they could consider the following considerations[3]:

- **Threats are global and therefore, solutions should be global:** Cyber threats know no borders; therefore, public and private sector should seek to cooperate and work together across borders and across sectors in order to most effectively combat threats.
- **The opportunity cost of compliance:** Complying with diverse, regional regulations, especially for firms that operate in multiple jurisdictions or provide services for multiple financial instruments, is complex, costly, and diverts resources away from actively securing the organization. This problem is compounded by the dearth of global cyber talent.
- **Inefficiencies of compliance:** Regulations in different jurisdictions often overlap and at times contradict each other. Additionally, regulatory requirements sometimes may even force institutions to make structural changes that might not be optimal from an overall business perspective[4].
- **The cost of fragmentation:** Localized solutions create operational risks which creates instability due to a more complex support environment. Typically, these solutions also result in suboptimal client experiences as banks have to build separate mechanisms for regional clients.

[2] FSI Insights "Regulatory approaches to enhance banks' cybersecurity frameworks", August 2017

[3] As the FSB notes in its "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices" (Oct. 13, 2017), seventy-two percent of jurisdictions plan to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year.

[4] For example, separating networks in different jurisdictions to avoid requirements that might be applicable to one subsidiary might be extended to the holding company or to other subsidiaries.

DEFINING REGULATORY FRAGMENTATION

Cyber-related regulatory fragmentation occurs when financial institutions must comply with different regulations in the same or in different jurisdictions that are similar (but not identical), conflicting and in some cases well-intentioned, but do not actually enhance cyber-resilience. All this might be a consequence of differences in their approach (rules-based versus risk-based), in the way that terms are defined or even fundamental cultural or regional differences around the usage and sharing of data.

Fragmentation is a considerable concern to the financial services industry, especially for firms that operate in multiple jurisdictions. Complying with myriad regulations and guidelines is complex, costly, reduces economies of scale, thereby making financial institutions less competitive, and diverts resources away from other effective cybersecurity related activities. Rather than enhancing overall cyber-resilience, uncoordinated regulations can pose a risk to financial stability.

The Financial Stability Board "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices" (the FSB Stocktake[5]) presents evidence that regulatory fragmentation is occurring across G-20 jurisdictions. To help illustrate the issue further, here are a number of current examples:

- **Incident reporting:** Institutions that experience a significant data breach in the European Union (E.U.) may potentially have to report the incident to regulators identified in the General Data Protection Regulation (GDPR), the Directive on security of network and information systems (the NIS Directive) and the Payment Services Directive II (PSD2) as well as to the European Central Bank. Additionally, there might be other national European regulations imposing similar requests. In the US case, 50 States have issued their own breach reporting rules, which are often similar but not the same. These disparate requirements create unnecessary burdens to the extent that the definitions and taxonomies used for each approach to reporting are not aligned. This concern can be addressed by creating a common lexicon and taxonomy for reporting incidents that can be used globally, either under any of those European regulations or also through the U.S. NIST "Framework for Improving Critical Infrastructure Cybersecurity" or possible future such requirements coming from SWIFT, TARGET 2, etc.

- **Sharing classified detailed threat information**: This includes all types of information sharing; enterprise-wide, bank to bank, bank to government and government to government, and it poses several challenges due to confidentiality issues, legal constraints, existence of international agreements (or lack of them) in place, etc. Additionally, there are different points of view as to what type of platforms (public-private vs private only platforms) are more appropriate, and the various degrees to which banks participate in the public-private platforms due to different sensitivities as to the objectives or the lack of feedback to institutions about reported information, usefulness and consequences of sharing information on those platforms. While the public sector can share classified contextual information with private sector individuals who have the adequate security clearance, those individuals can often only take limited action (for example share with relevant colleagues) due to restrictions. This is a critical issue for global financial services firms, as they represent a significant portion of the financial sector's critical infrastructure and need access to classified threat information in a timely manner. Governments could consider best practices from the U.S. such as granting temporary clearances. Additionally, sharing indicators of compromise is often insufficient to inform private sector incident response efforts. For example, at times, quickly sharing full malware samples instead of derived indicators and analysis will be key. Governments and regulators should explore tools to share detailed threat data, including malware samples and contextual information, while protecting privacy and firm-specific identifiers.

  While good information sharing can detect patterns and trends to enable organizations to better guard against cyber-attacks and other incidents, it is up to governments and regulators to provide assurances to the industry concerning the

5 See; "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices", October 13th, 2017.

subsequent use of such sensitive and confidential information given the potential risks to reputation, market confidence and liability. For example, exploring liability protections, such as providing a safe-harbor from civil, regulatory and antitrust liability, is a minimum necessity.

- **Use of cloud services.** This practice is becoming increasingly important for firms, not only in terms of defining their business model but also for cybersecurity purposes, given that many firms rely on cloud providers to provide high levels of security against cyber-attacks. However, the way in which rules around the use of cloud computing are developing, may produce asymmetries and level playing field issues. As an example:

    - The criteria applied by competent authorities to allow the outsourcing of services to the cloud are not homogeneous in all jurisdictions[6][7].
    - Depending on jurisdictional regulations about geolocation of customer's data, the ability to use the cloud might not be the same for all institutions.
    - In Europe, the Outsourcing Directive has been transposed to national laws whereby the Central Bank or the European Central Bank needs to acknowledge the outsourcing of data to cloud providers and where national data protection regulators are also involved in validating security controls. There are occasions where the central banks are questioning or requesting additional information of the security controls used with the Cloud Service Providers (CSP), when these controls have previously been validated by the national data protection regulators. Additionally, the E.U. NIS Directive which affects financial institutions and CSPs might also potentially result in further overlap.

- **Data protection regulations.** Data is one of the most precious commodities and is a common target of cyber-attacks. Rules around data protection might conflict/not be fully aligned with other regulations or initiatives, as it is shown in the following examples:

    - The E.U.'s new "General Data Protection Regulation" (GDPR)[8] requires institutions to protect the personal data of their customers, whereas the PSD2[9] obliges them to facilitate the access to that personal data, thus creating another potential entry point for data breaches or fraud. The goal of PSD2 is also to increase competition, lower cost, and foster innovation in the payments system, and to do so, payment providers in general and also account information aggregators will have direct access to bank accounts, making them an easier target for hackers than banks themselves but with as much information.[10] Additionally, and to foster competition, PSD2 limits banks' ability to make discriminatory judgments or impose contractual obligations on them around providing the same level of protection for sensitive customer information than banks, so there are not real incentives for those new players to do so. Finally, monitoring for fraud might become much harder, among other things because clients would not interact with banks directly, so monitoring their behavior would become more difficult.
    - Incident sharing could be more effective revisiting what information could be shared, including personal data such as IP addresses. Currently, in some jurisdictions that information cannot be shared, but it would significantly help mitigate or limit the effects of DDoS or phishing campaigns. As an example, having the possibility from a legal and practical perspective to share more data among banks cross-jurisdictionally and then applying data science to it could enhance the effectiveness of detecting and stopping cyber-attacks and other incidents.

---

[6] See Enisa report: "Secure Use of Cloud Computing in the Finance Sector", December 2015.

[7] See Asia Cloud Computing Association report: "Asian Financial Services: Ready for the Cloud" (http://www.asiacloudcomputing.org/images/research/ACCA_Report_-_Web.pdf)

8 E.U. General Data Protection Regulation. See: https://www.eugdpr.org/

9 E.U. Payments Services Directive 2. See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

[10] See FT article: "Why would we want to increase the cyber risk to our bank data? " https://www.ft.com/content/4911d260-aaac-11e7-ab55-27219df83c97

- Geolocalization requirements pose some concerns. For example, GDPR forces to geo-localize data within the EU and only allow its transfer by using Model Contractual Clauses, Binding Corporate Rules, or special agreements between countries such as the Privacy Shield. In other jurisdiction these requirements also vary, ranging from the ones that are even stricter and disallow or limit data transfers outside of their countries, to those ones that require in-country initial collection and storage of data (for AML purposes for example) and then allow to share and store it elsewhere.
- The legal responsibilities of entities in a data breach is also unclear. Breaches may very well happen through the supply chain that services banks (including fintechs that have access to bank data, or aggregators as mentioned above), but often it is unclear who is ultimately responsible for the protection of the data.

- **Penetration-testing:** This practice is an important tool of a robust security assessment program, and it is critical that public and private sectors work together, to understand drivers, focus approaches and requirements. In this vein, we fully support the industry-developed GFMA framework on "Regulatory-Mandated Third-Party Penetration Testing,"[11] where they underscore the potential adverse consequences of the lack of a unified approach to pen testing, which include:
  - Multiple regulatory frameworks can result in unnecesary duplication of sensitive information, putting financial firms, their clients, and other downstream third-parties at unknowable risk.
  - Testing insights are reduced when regulators narrow options around test personnel and testing methods.
  - Increasing regulatory requests requires testing teams to spend more time complying with requests, and less time testing operational controls.
  - Multiple regulatory frameworks can result in inconsistent reporting.
  - Penetration-testing of critical systems in production creates the significant potential to disrupt firm operations.
  - Creating multiple one-size-fits-all penetration-testing frameworks disproportionately impacts mid-size and smaller financial institutions.

  In some instances, where an institution has demonstrated sufficient understanding and capability, that institution should be able to administer its own penetration-test. That is the case in the US, and recently, the Bank of England is understood to have signaled its openness to its CBEST penetration-testing program to allow for "firm led" testing under certain circumstances. However, the Hong Kong Monetary Authority requires an independent penetration testing.

- **Governance.** In some jurisdictions, like the E.U., there is a strong recommendation from the Supervisor that the Board of Directors oversee the governance of cyber-risk, whereas it is not the case in other jurisdictions. There should be clear governance assigning roles and responsibilities, but financial institutions should be given the freedom to determine how to put it into practice. Boards should be informed but should be able to decide, for example, to delegate that oversight function to a Committee.

Additionally, financial institutions and regulators need to be attentive to possible future sources of fragmentation. For example:

- Different regulatory approaches that some jurisdictions are taking towards the cyber-risk related to new technologies (blockchain, artificial intelligence, etc).

- Different certification and attestation initiatives, which are being proposed to help provide assurance regarding the cyber-resilience of the value chain of institutions. For example, the current cybersecurity legislative package of the E.U. introduces a cybersecurity certification act, that is raising awareness within and outside Europe, including with Cloud service providers and other essential digital services, around what optimal certification scheme approaches. Since there

[11] See GFMA website: http://www.gfma.org/correspondence/item.aspx?id=827

are different certifications both at the global and national levels, there might be a point where a certification that is valid in Europe, may not be in other jurisdictions, or vice versa.

ADDRESSING REGULATORY FRAGMENTATION

Regulatory fragmentation could be addressed by designing a global regulatory landscape for cyber-risks that enhances both the cyber-resilience and stability of the financial sector. In doing so, it should be noted that not all cyber-risk related topics require the same regulatory approach.

In general, the incentives of financial institutions and regulators (and other public-sector institutions) are aligned: including the desire to reduce or eliminate the risk of successful cyber-attacks and other incidents, protecting financial stability, improving the posture and resilience of financial institutions on cyber-risk, and to operate in a cyber-resilient environment, among others. Each institution being more cyber-resilient means that the whole financial system is more resilient, and that includes all its constituents regardless of their size. Given the aligned incentives it would be appropriate to develop flexible and efficient approaches that optimize practical solutions over prescriptive measures.

The framework

For achieving that, a common globally accepted risk-based, principles-based framework would be useful and sufficient. Such a framework, without being overly prescriptive, could be the foundation for designing, managing, analyzing, and evaluating the cyber-resilience of financial institutions, and to promote international cooperation and information sharing. At the same time, this would help in building trust among organizations, governments and with the public. To some extent this is already happening, as noted in the FSB Stocktake "All FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies in developing their cybersecurity regulatory and supervisory schemes for the financial sector." This underscores that there is already some degree of international convergence, but more needs to be done.

Arguably, some existing frameworks provide a good basis for defining and implementing a cyber-strategy within each financial institution as well as the governance that help that strategy, and to address the challenges that cyber-risks pose, the protection of data or even the promotion of international information sharing, which goes a long way in dealing with a threat which is global in nature.

In this regard, the industry supports the FSB in creating such common framework, very closely based on the U.S. NIST "Framework for Improving Critical Infrastructure Cybersecurity." Indeed the FSB already concluded in its 2017 Stocktake that "in developing their cybersecurity regulatory and supervisory schemes for the financial sector, all FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies."[12] This small body includes the U.S. NIST Framework, as well as 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), and the International Organization for Standardization 27000 series. "This suggests that jurisdictions have found the existing guidance and standards to be useful in developing their own schemes and that there is some degree of international convergence in cybersecurity regulation and supervision of the financial sector."

[12] See FSB "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices" (Oct. 13, 2017.)

It should be noted that that the U.S. NIST framework, which has been embraced by many financial services firms around the world, is consistent with the G-7 Principles[13] and the CPMI-IOSCO Guidance. The NIST framework is also consistent with some of the principles that the industry believe are important to follow. Those principles are:

- The framework should address cyber-risk from a risk management perspective with the objective of promoting the cyber-resilience of institutions in a broad sense:

    - Cyber-risk should be part of the general enterprise risk management (ERM) program of institutions with a focus on: the types of relevant cyber events for the institution, magnitude of possible impacts, assessment of the criticality of the different assets of the institution from a cyber-risk perspective and hedging through insurance, among other factors.[14] However, cyber-risk is a non-financial risk that is different from the other more traditional financial risks (namely market risk and credit risk) in that cyber-risk is usually "intentional" in nature, there is limited public data about the number and severity of events, and the impact is hard to quantify given the high level of interconnectedness of the financial system. Attackers are looking actively for vulnerabilities to exploit and impacts usually do not conform to statistical patterns, making valuation very difficult if not impossible. For the same reason concepts such as "risk appetite" should be rethought for this risk.

    - Having a clear and transparent governance of cyber-risk within institutions is key for cyber-resilience, and the framework should cover the governance of all the basic cybersecurity functions (identify, protect, detect, respond, and recover).

    - Top management involvement in cybersecurity is essential, as it defines the posture of the institution on cyber-risk, whether to have a more proactive approach to cybersecurity versus passive, to what extent strategic decisions are informed by cybersecurity factors, etc. The framework should emphasize this aspect without being overly prescriptive as to how to achieve it.

- The framework should be based on principles. As discussed before, as the incentives for institutions and regulators are aligned to a great extent, there is not always a need for hard rules. That would create cost inefficiencies and those rules could become obsolete in a short period of time, also given the speed of technological developments.

- The framework should recognize that financial institutions are at different stages in their overall development towards cyber-resilience, so it should allow for progressive improvement towards the leading practices in the framework.

- The framework should be addressed to, and be relevant for all market participants in the financial system, including banks, insurers, asset managers, financial market infrastructures, their regulators and supervisors, third party vendors, cloud providers, and all those other companies and fintechs that perform financial activities (payment platforms, lending platforms, account aggregators, hedge funds, money market funds, etc.) Because of the way cyber-attacks and other incidents work in a highly interconnected industry, where attackers always look for the weakest link in the chain, it is not enough to consider only financial institutions but any other entity that is part of the financial ecosystem.

- In the same vein, and because cyber-risk has some characteristics that make it different from financial risks, trying to apply the principle of proportionality (either according to size, complexity of business model, interconnectivity, systematically, etc.) does not make sense. They all must have a governance in place to identify, protect, detect, respond and recover from cyber-events, although the implementation of that governance may vary from institution to institution. A successful cyber-attack on any component of the financial ecosystem could potentially spread into other parts of the financial system given its interconnectivity.

[13] See the "G7 Fundamental elements for effective assessment of cybersecurity in the financial sector"
[14] See IIF Cyber-risk Insurance paper at https://www.iif.com/system/files/32370132_iif_cyber_insurance_paper_12_04_2017.pdf

- The framework should encourage local regulators, when developing their standards, to do so in coherence with the overarching framework and with other existing relevant international standards, so that regulatory fragmentation contained where possible.

Other Regulations

Achieving a globally-accepted framework would be an important starting point for addressing regulatory fragmentation. There are other cyber-related topics where incentives may not necessarily be fully aligned, and where respective jurisdictional sensitivities may inspire divergent approaches. In those cases, they should ideally be developed upon or in coherence with the overall globally accepted framework, and maintaining sufficient flexibility to be useful in a rapidly changing cyber and technological environment. In many cases, those approaches could be based on principles, as prescriptive rules can quickly become outdated.

Some of the topics where incentives might not be aligned include data protection, data ownership or data localization laws, communication of cyber-attacks and other incidents to authorities, and supervisory-led penetration testing.

Data is one of the main critical assets that institutions have, so the main goal should be to keep data safe, available, and un-corrupted, especially given the potential economic consequences of reputational loss that a breach could pose to the financial institution and to the sector as a whole. Achieving that normally involves a strong governance system, but imposing rules with strict recovery times, tight communication periods to authorities and/or incumbents, prohibition to share information across jurisdictions, and imposing significant fines are all requirements that need be well balanced. For example:

- Recovery times should account for the fact that sufficient time has been allowed to properly check that systems are no longer compromised, and this time can vary with the circumstances.
- In some instances, limitations to share information internationally about cyber-incidents can be detrimental to an effective response to the threat and to mitigating its consequences.

When it comes to the need to communicate incidents to authorities and regulators (incident reporting), their objectives and the ones of institutions might not be always aligned. For example:

- To respond to a successful cyber-attack, the main objective of financial institutions is to resume operations as swiftly and safely as possible, whereas authorities might want to track down the attackers to bring them to justice. That sometimes means leaving the vulnerability open on purpose, with obvious consequences for the institution. Here again a constant and constructive dialogue is needed.
- When a breach occurs in an institution, different authorities and regulators request to be informed directly by the entity following their own rules, whereas the entity would rather keep this reporting to the minimum necessary. In this case solutions such as “one-stop-shop mechanism” for financial institutions with regards to regulation could be envisaged, so that there is only one institution (such as the home supervisor) in charge of centralizing all the requests from the different regulators and supervisors within each jurisdiction (including host supervisors), and maybe as well as across jurisdictions. This could encompass centralizing data breach reporting or any other type of ICT audit, certification requested by other regulators or authorities, etc. Supervisory colleges could play a unique role in sharing these developments in a consistent and timely manner.

Another example where objectives are not aligned is with regards to information sharing:

- For the private sector, cybersecurity includes financial, operational and reputational risk, fitted to a business model built around profit margins and shareholder interests. Sharing information raises concerns regarding regulatory consequences, penalties, and exposure to legal actions. There is a need for comfort and protections regarding exactly who is sharing information, what they are sharing and who will see that information. Additionally, the private sector has to consider how to protect privacy and personally identifiable information (PII), competition with peers (where reporting vulnerabilities may damage commercial interests), anti-trust laws, trade secrets, and other sensitive information. There are also considerations regarding supply chains, partners and third party vendors.
- For the public sector, cybersecurity is about a common public good, including finnacial stability. While issues regarding the data shared and who see it exist, the regulatory and reputational risks are not the same.

- For private-sector security firms, their business model is reliant on obtaining, holding and selling information, not sharing it.

CONCLUSIONS

Cyber-related risks are gaining momentum and have become one of the top priorities for financial institutions, regulators, supervisors, and other authorities alike, and it is key that the related regulations facilitate, promote and contribute to enhancing the cyber-resilience of the financial sector and effectively reducing the risks to financial stability. For doing that it is welcome that the G-20 and other authorities design a global regulatory landscape, which could include:

- A globally harmonized and comprehensive principles-based and risk-based regulatory framework for cyber-risk. Jurisdictions could then be encouraged to align their regional and national regulations, guidance and supervisory practices towards this framework.

- The identification and analysis by the Financial Stability Board, at the behest of the G-20 and together with other authorities of the leading practices that are most successful in strengthening resilience and mitigating cyber incidents. Those leading practices could be promoted and adopted across jurisdictions to avoid fragmentation. They could address, among others, the following priority topics:

    - Approaches to penetration-testing exercises
    - Practical and efficient ways of collaboration between private and public sector
    - Development of a common language and taxonomy for reporting purposes
    - Analysis of ”one stop shop” mechanisms for financial institutions with regards to regulation to centralize all cyber-related requests, including breach reporting.
    - Cybersecurity certifications and attestation initiatives.
    - Re-think the role of supervisors and their assessment of the financial sector cyber-resilience.
    - Dialogue among home and host supervisors regarding the cyber-resilience of international financial institutions.

- Promote industry initiatives like the “Financial Sector Profile”, which synthesizes globally-accepted cybersecurity principles, including those in the NIST Framework, G-7 Principles, and CPMI-IOSCO guidance. It uses a common vocabulary and taxonomy by which the financial services sector regulators and industry can communicate with each other to establish a common understanding of any financial institution’s cybersecurity posture.

- Support initiatives like the one of the FSB on producing, as a first step, a lexicon to help support consistent terminologies across jurisdictions, which is very relevant given the lack of common definitions around various terms related to cyber-resilience from a financial services perspective. This initiative could also benefit future FSB work around the common framework proposed in this paper.

- Increase the efficiency of the financial sector when fighting against cyber-attacks and other breaches by promoting the necessary changes in legal frameworks that might act as stoppers or bottlenecks in doing so. Issues such as cross border government to government, government to bank, or bank to bank information sharing, any restrictions should be re-thought for cybersecurity purposes. The goal of information sharing for the purposes of addressing cyber-risk and the safeguarding of proper privacy protections are not mutually exclusive.

- Address new risks arising from critical national infrastructure, outside the regulated financial industry. The management of cybersecurity by third parties and non-financial infrastructure sectors is essential. Financial institutions, governments and regulators should engage them to identify risk aggregation, evaluate their service provision and encourage them to provide information on their cybersecurity programs. This should not be about the creation of any new obligations that may pose a significant compliance burden. However, rationalizing and bringing more coherence to any form of reporting, information sharing and aggregation is desired. Ensuring third parties develop a greater understanding of the regulatory expectations

and pressures of the financial institutions that they serve would benefit the entire industry and promote the development and update of cybersecurity frameworks and norms.

In all those regards, international standard setters and other authorities are in a privileged position to lead further efforts to better shape the global regulatory landscape, to reduce regulatory fragmentation, and to encourage jurisdictions to follow that lead.