International Cybersecurity, Data and Technology Principles

Introduction

A strong, open and resilient technological ecosystem is essential to the health and protection of financial markets. Increased reliance on and use of technology creates benefits, but also engender inherent risks. Those risks, both to technological infrastructure and financial stability, require responses from regulators and government agencies, and we applaud governments for paying closer attention to this critically important issue.

It is also important, however, that countries and jurisdictions tackling risks do not create rules that inadvertently force global businesses to fragment their technology systems, impeding competition and innovation, thereby harming investors. This fragmentation would not only impede the flow of global capital and its contribution to economic growth, but also exacerbate the very risks regulators are trying to mitigate.

Countries everywhere are grappling with these new and intrinsically global challenges. We therefore believe that a conversation between policymakers, industry and other interest groups needs to take place at an international level to ensure that policy remains effective and that the global economy benefits from the full promise technology stands to offer. In the interests of helping begin that conversation, the Securities Industry and Financial Markets Association (SIFMA), Asia Securities Industry and Financial Markets Association (ASIFMA), European Banking Association (EBA) and International Swaps and Derivatives Association (ISDA), have outlined a set of principles we believe are essential for the formation of effective policy on cybersecurity, data and technology.

The purpose of these principles is to capture and proactively share the considerations that should be taken into account when a nation or one of its agencies or standard-setting bodies creates laws, regulations, or standards that affect the technology infrastructure of financial services firms operating globally. The principles are not exhaustive and are mainly a means to establish a conversation.

We are therefore reaching out to the Financial Stability Board (FSB) and the International Organization of Securities Commissions (IOSCO), each uniquely positioned as international standard-setting organizations, to seek their views and guidance in this process.

Global Environment

There are two crucial issues that must be recognized before principles for effective policymaking can be established.

First, cybersecurity, data protection and technological advancement are international issues requiring global solutions. Global systems play an important role for financial institutions to promote security and innovation, while mitigating risk. Such risks transcend national borders, so

countries – through governments and private sector institutions – need to work together to develop safeguards that protect the integrity of global markets.

The financial sector is subject to significant and diverse laws, regulations and examination standards related to financial technology, data protection and cybersecurity that reflect an emerging international consensus on what is most effective. In some important cases, standards are being established at the international level. For example, the Payment Card Industry Data Security Standard (PCI-DSS) is a global industry standard that sets security requirements for all the payment card systems financial institutions use. Thus, the use of internationally accepted standards can minimize the risks for global financial networks by ensuring that best practices are widely implemented. Adopting such global standards also avoids the problem of asking international firms with global platforms to comply with conflicting rules and regulations in individual markets. To that end, we urge the FSB and IOSCO to adopt our goal of avoiding the exclusive use of localized solutions, prescriptive technologies and onerous restrictions on data flows.

This international perspective is, for example, crucial in crafting policy on encryption standards. Local encryption standards are sometimes inconsistent with international practices which could raise security concerns for companies and international regulators. Adapting internationally accepted approaches to encryption – such as those used in Singapore and the United Kingdom – minimizes conflicts across systems in different countries and ensures that client data is as well-protected as possible – something that globally recognized industry regulations require as well.

Similarly, requirements to disclose source code are problematic in a globalized economy, which is one reason they are not a feature of prevailing rules and regulations in most markets. Internationally-accepted standards on software and intellectual property (IP) licensing typically preclude banks from disclosing or holding third party IP in escrow without permission from the owners (or licensors) of that IP. Such disclosure would expose firms to unquantifiable financial risk from litigation, and IP actions by software and IP licensors for breach of standard controls and contractual provisions protecting supplier IP.

Second, cybersecurity threats, risks, and the technology that mitigate them shift faster than regulations and standards can respond. Current threats to data, assets, and the overall strength of the financial markets include: (1) independent criminals (e.g., for account manipulation or data disruption); (2) nation-states or terrorist groups (e.g., for damaging the financial system or espionage); (3) hacktavists (e.g., for political gain); and (4) insiders (e.g., abusing access by harvesting customer information). Regulators may also promulgate well-intentioned but misaligned regulations, causing inefficient use of resources for financial market participants. National governments may enact laws and regulations that unintentionally undermine privacy, national secrets and economic growth. For example, sharing of data is essential to detecting cyber crime incidents, but these activities can be precluded by onerous data protection rules. We encourage proactive interaction between governments, regulators, and industry participants.

Policies that require specific technology requirements, detailed technical reviews or other processes by regulators will be reactive to the threat environment and to adversaries that seek to take advantage of vulnerabilities. In addition, embedded regulations and prescriptive standards

can become quickly outdated as cyber risks and the technology that addresses them evolve. This fast-changing threat environment, coupled with rigid technology solutions, can create obstacles to protecting financial institutions and their clients. As policymakers in a number of markets have already recognized, effective regulations go beyond assessing whether an institution is compliant with a particular standard and instead ensure that sufficient people, processes and technology are in place to manage risks.

Principles for International Cybersecurity, Data and Technology

Given the global and constantly evolving nature of technology, we encourage the FSB and IOSCO to base their policies and standards regarding cybersecurity, data and technology on the following high-level principles to promote workable and effective global regulation and governance.

- Support technological innovation and the unrestricted choice of technologies to enable business objectives and data and system protection policies.

- Encourage the development and use of financial technology ecosystems that are open, safe and interoperable with an understanding that each financial services firm and its associated partners are necessarily dependent, linked and able to affect each other within this global ecosystem.

- Encourage the use of existing standards and frameworks by financial services firms, their business partners, vendors, and regulatory agencies in order to provide a foundation for globally synchronized regulatory approaches.

- Recognize the ability to transmit data across national boundaries and the storage of that data in countries other than the ones within which it was created is fundamental to supporting a global financial system that is capable of enabling the goals of national economies and the industries that comprise them.

- Standards, guidelines and regulations should be created in an open and transparent process that encourages consultation and collaboration between developing bodies, those required to adopt the new policies, and other affected stakeholders.

- Regulators should add value by evaluating policies, procedures and operational results, not the technical details and intellectual property of software, or the technologies enabling these programs.

- Cybersecurity is a shared responsibility requiring proactive and reactive action on the part of national governments, regulatory agencies, financial services firms, partner businesses, and individual employees and customers; all have the ability to favorably and adversely impact each other.

- Recognize that there is no one-size-fits-all approach to cybersecurity and that regulations should enable programs that are risk-based, threat-informed, and based on the size, scope, function and business model of the entity being regulated.

- Acknowledge that cyber risks are just one component of enterprise risk management. They are both unique and different from other risks, but at the same time similar in that they cannot be eliminated, only managed based on the risk appetite of the firm.

- Firms must strike a balance between security and privacy based on their obligation to maintain the privacy of their customers' data, but at the same time monitoring customer and system activity to ensure their networks are secure and operating within the law.

- Support approaches to operational assessments which are safe, globally scalable and risk-based, so as to reduce negative impacts on operations and avoid creating new risks.

Conclusion and Next Steps

The best approach for developing technology policies is open and transparent formulation and implementation, which allows stakeholders to provide meaningful input to regulators. This helps ensure that the resulting regulations are effective, compatible with global norms, and unlikely to cause unintended consequences. In particular, effective prudential frameworks and policies must allow companies to conduct their own risk assessments and determine what technology best meets their security needs.

These principles are an attempt to capture considerations that should be taken into account when a nation or one of its agencies or standard-setting bodies creates laws, regulations, or standards that affect the technology infrastructure of financial services firms operating globally. There are also additional plans to circulate these principles more broadly.

We respectfully urge IOSCO and FSB to take these principles into account when engaging in policymaking, and standard-setting activities, to better ensure that financial systems around the world address the risks that may cause the most harm and are as secure as possible. We hope to be able to cooperate with both organizations, and with others, on this issue going forward.

Asia Securities Industry & Financial Markets Association (ASIFMA)

European Banking Federation (EBF)

International Swaps and Derivatives Association (ISDA)

Securities Industry & Financial Markets Association (SIFMA)