Cyber Security & Financial Stability:

How cyber-attacks could materially impact the global financial system

September 2017

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

Cyber-attacks are growing rapidly and pose a substantial risk to the stability of the overall financial sector. Attacks are increasing in number, scope, and sophistication, making it difficult to predict the total impact. The Herjavec Group has predicted that the global annual cost of cybercrime is estimated to increase to around USD 6 trillion by 2021, from USD 400 billion in early 2015.[1] Similar estimates can be found by organizations such as Juniper Research and the World Economic Forum, and in a July 2017 report, Lloyd's of London estimates that a single global cyber-attack could result in damages of as much as USD 121 billion.[2] Beyond financial loss, cyber-attacks can disrupt business, financial markets and contribute to a broader loss of confidence.

The modern world is rapidly becoming more digitalized, reliant on data and increasingly interconnected. Cyber-attacks can impact all segments of life, as evidenced during the global WannaCrypt ransomware attacks in May 2017 that affected more than 200,000 computers in at least 150 countries, including those found within hospitals, utilities, railways, telecommunications and automobile companies; as well as the more recent June 2017 Petya ransomware that impacted computers within 64 countries. While the impact of the recent ransomware attacks on financial institutions was limited, the financial services sector has traditionally been the largest target due to both the attractiveness of financial gain and access to confidential financial data. According to IBM, the financial sector in 2016 was attacked 65% more often than any other sector, resulting in more than 200 million records being breached, a 937% increase over 2015 when just under 20 million were breached.[3]

Banks and other financial institutions are increasingly concerned about the sharp increase in cyber-attacks and their consequences. In an IIF survey of global banks, conducted in partnership with EY, both the Boards of Directors and Chief Risk Officers (CRO) deemed "Cyber-security" to be a top strategic priority, second only to addressing new regulatory rules and supervisory expectations.[4]

Cyber-attacks are increasing sharply and the financial sector has traditionally been the largest target.

This paper analyzes the relationships between cyber-attacks and overall Financial Stability, including transmission channels and the types of scenarios that could have systemic repercussions, including:

- **Attacks on financial market infrastructures**
- **Corruption of data**
- **Failure of wider infrastructure**
- **Loss of confidence**

It also reviews what measures financial institutions and the public sector are already undertaking, and what more could be done to identify, address and mitigate threats to overall financial stability.

[1] Herjavec Group / Cybersecurity Ventures "Hackerpocalypse: A Cybercrime Revelation" Q3 2016; See also Juniper Research "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation" May 2015; and World Economic Forum "Global Risks report 2016." Jan. 2016.

[2] Lloyds's of London. "Counting the cost: Cyber exposure decoded." 17 July 2017.

[3] IBM "Security trends in the financial service sector." April 28, 2017.

[4] EY/IIF "Seventh annual global bank risk management survey." Oct. 12, 2016.

Individual financial institutions have been investing heavily in control functions to counter these threats, increasing risk awareness and safeguarding critical assets and data. Authorities, in turn, have developed strategic initiatives, guidance papers and regulatory approaches to combat cybercrime and to strengthen the resilience of the wider financial system. There are also various initiatives being developed around the world that promote intelligence gathering and information sharing between public and private sector stakeholders (which, together with data, are pre-requisites for cyber-insurability).

But due to the global nature, importance and interconnectedness of the financial system, and the sharp rise in cyber-attacks, there has been an increasing focus on what impact such attacks could have not only on individual institutions but also the stability of the overall financial sector.

FINANCIAL INSTITUTIONS AND CYBER-RISK

Over recent years, the types of perpetrators of cyber-attacks have expanded and their skills and sophistication have significantly increased.

These perpetrators can belong to hacking groups or to criminal gangs but they may also be state-sponsored[5] as part of a broader and more powerful attempt to destabilize other jurisdictions by, for example, disrupting their networks (i.e. electricity) or infiltrating their systems (i.e. communications system, financial system, etc.)

One such example is North Korea, which is alleged to have sponsored several attacks, including both the already mentioned WannaCrypt ransomware and the attempted heist of USD 1 billion from the Bangladesh Central Bank[6]. in February 2016. According to TIME, North Korea employs an army of 6,800 state hackers that generate an annual revenue of USD 860 million.[7] Their mission is both to cause physical or economic damage to their targets, and to obtain revenues to help finance their nuclear program.

The motives of perpetrators vary widely, but could be organized into four broad categories:[8]

- **Cyber-crime**: the motivation is a financial gain (e.g. attacks that seek to steal money);
- **Cyber-espionage**: gain information on another organization in pursuit of leverage (e.g. political, financial, capitalistic, market share, etc.);
- **Cyber-hacktivist**: involves stealing information to serve a political agenda; and,
- **Cyber-war**: the notion of a nation-state's effort or transnational threat to compromise/coerce an adversary via a cyber-attack.

Regardless of the actor, the tools used or the motives they might have, any attack on critical components or services of the financial system, could have either direct or indirect impacts that could threaten the stability of the system, or of its respective participants. For this reason, the threat of cyber-attacks is no longer an IT or operational risk within financial institutions, and has expanded into broader more holistic categories, such as "enterprise risk" and "system wide risk."

Examples of recent cyber-attacks on financial firms:

- **2012: The Distributed Denial-of-Service (DDoS) attacks on five large U.S. banks, with damage in the form of lost business;**
- **2013: A South Korean bank hack that disrupted financial networks and impacted ATM's bringing commerce to a standstill for several days;**
- **2013-2015: The Carberp Trojan, where more than one billion dollars were stolen from banks around the world over those two years;**
- **2014: Data breach attack on a large U.S. bank, where the data of several million customers were compromised;**
- **2016: Hackers stole USD 81 million from a Bangladesh bank, penetrated through a messaging system; and,**
- **2016: Indian banks data breach, where 3.2 million debit cards were compromised.**

But unlike financial risks, such as credit or market risk, and given the novelty and constantly evolving nature of cyber-attacks and the lack of empirical data, cyber-risk cannot easily be modelled, measured, or hedged based on past performance, as can be done with credit risk, for example.

[5] See for example Reuters, February 15th, 2017: "Ukraine charges Russia with new cyber-attacks on infrastructure."
[6] See Reuters, May 19, 2016.
[7] See TIME magazine, May 16, 2017.
[8] See the comments by Richard Clarke, for example, at "Oracle Industry Connect" in Orlando, FL on April 13, 2016.

Financial institutions are already employing many measures to reduce the impact of cyber-attacks, including: having a good understanding of cyber-resilience, adopting a comprehensive and forward looking approach to manage cyber-risk, implementing the right controls and responsive actions available for mitigating a security failure, and engaging in swift cyber-threat information sharing.

The transformation process that financial institutions, financial markets and financial infrastructures are undertaking to adapt to the new "digital future" will exacerbate cyber-risks. This can be seen, for example in:

- The increased number of processes, some of them critical, that banks are outsourcing to third parties, sometimes across borders;
- The more common use of the cloud for data or computing purposes;
- The increased interconnectivity with customers through multiple channels;
- The increased use of robotics or algorithms for automatic trading and the development of application programming interfaces (API); and,
- The increased use of virtual and digital currencies.

All the improvements and opportunities from the broader developments in digitalization also enable more possible platforms for cyber-criminals to target and exploit.

Given the increase in attacks, it is essential that the financial system enhances cyber resiliency through the individual action of financial institutions and through increased coordination across participants, including the sharing of information and developing a set of commonly understood sound practices that could be supported and enhanced by the public sector. In this respect, initiatives like the FS-ISAC (Financial Services Information Sharing and Analysis Center[9]), the recently created FSARC (Financial Systemic Analysis and Resilience Center), and the SABRIC (South African Banking Risk Information Center), are already playing a crucial role in facilitating intelligence gathering and information sharing in various jurisdictions around the world. However, not all financial institutions participate in these initiatives. Some institutions prefer to exchange information privately, while others only exchange non-sensitive information. Furthermore, certain organizations are restricted by law as to what information they can share, there are also overlaps between different laws requesting reporting of incidents using different taxonomies and thresholds. As such, these models should be analyzed with a view to remove any friction that hinders information sharing Going further, collaborative efforts need to include contingency planning and exercises to increase effectiveness in response to attacks.

FINANCIAL STABILITY IN A CYBER CONTEXT

The stability of the financial sector is crucial for the economy. The 2008 financial crisis put financial stability to the test and in a number of jurisdictions the public sector had to provide support to prevent the failure of large financial institutions. Consequently, a wide range of global post-crisis reforms were proposed to safeguard the system, including greater capital and liquidity requirements as well as effective resolution frameworks to ensure bank failure is addressed in an orderly fashion.

However, these measures do not address the core factors of cyber-risks. Cyber-attacks are a threat to financial stability not only through their impact on one institution, but also through their impact on multiple components of the financial system (see below) or through the indirect impact on an essential utility provider, such as an electricity or telecommunications provider, which may have the same, or even larger, negative impact. There is therefore a growing concern that a cyber-attack can result in a systemic event, which could be much more difficult to manage and control than the failure of a single global financial institution.[10]

The financial system is also broad and diverse, with many interconnected components that, if attacked, could further impact the other parts of the system. An overview of the main participants would include:

- **Banks**: including commercial banks, investment banks and central banks;
- **Non-bank financial institutions**: asset managers, insurance companies, finance and loan companies, mutual funds;
- **Other financial services**: credit card companies, payment service providers, investment funds;

[9] See the FS-ISAC website: https://www.fsisac.com/

[10] The need to protect national critical infrastructures from cyber-attacks is widely recognized in regulations like the "Network and Information Systems Directive EU 2016/1148" or the "Framework for Improving Critical Infrastructure Cybersecurity issued by the US NIST"

- **Markets**: stock markets, debt markets, derivatives markets, commodities markets, foreign exchange markets; and,
- **Financial markets infrastructure**: payment systems, central securities depositories, custodians, central counterparties, securities setlement systems, trade repositories, messaging systems.

All these components of the financial system are closely interconnected in often complex ways, and their underlying infrastructures are built to satisfy customer demands. Scenarios that destabilize the financial system are hard to predict. All the participants in the financial system, and especially those that provide critical services or that are systemically important, have very strong and well proven cyber-risks programs, controls and business continuity plans in place. However, if left unaddressed, a detrimental cyber-attack has the potential to de-stabilize the global financial system. The use of zero-day vulnerabilities[11] affecting broadly used infrastructure components such as operating systems may have such a systemic impact.

While most cyber-attacks do not have the objective of destabilizing the financial system, attacks motivated by financial gain and cyber-espionage can still have a dangerous and detrimental effect on the economy, as evidenced by the recent WannaCrypt ransomware attack.

Amongst the different types of cyber threats, cyber-hacktivists who aim to steal and manipulate data to serve a more political agenda and cyber-war, where large institutional powers seek to destabilize their adversaries' financial system with powerful and sophisticated attacks, are most worrying.

The U.S. Office of Financial Research (OFR), when reviewing how financial stability can be impacted, identified the following key drivers:[12]

- **Lack of availability**: the functions and services provided by many of the above-mentioned components of the financial system cannot be replaced easily if lost or interrupted;
- **Loss of confidence:** this is probably the biggest danger, as the whole financial system is built on the confidence placed by participants, and could lead to runs on short-term funding, liquidity freezes and defaults; and,
- **Loss of data integrity:** reliable, accurate real time data is key to the performance of the financial system, and the loss of that integrity could disrupt market activity significantly.

Building on these key drivers, some of the scenarios that could help illustrate the risks are the following:

POSSIBLE CYBER ATTACK SCENARIOS

Four scenarios are described where significant cyber-attacks, through various transmission channels, can lead to loss of confidence and/or loss of data integrity. In some scenarios, there is also the possibility of a lack of availability.

Such attacks could target banks, payment systems, financial market infrastructure, service providers, messaging and data providers, telecom and cable companies, and central banks and other public sector systems. The impacts from such attacks would be far-reaching, and could include: liquidity dislocation, credit losses, clearance and settlement disruption, threats to data integrity, loss of consumer confidence (bank runs), interrupted revenues and other materials costs to financial institutions and end users. Here are some possible scenarios:

Scenario 1: Attack on Payment Systems

A payment system is defined as any system used to settle financial transactions through the transfer of monetary value, and includes the institutions, people, processes and technology that make such an exchange possible.

Many payments systems are critical services that are usually provided by governments in cooperation with banks and other financial institutions. In the World Payments Report, it is estimated that in 2015 approximately 426 billion non-cash transactions were processed globally, with an increase of about 10% per year. [13]

Some payment systems have grown to a global scale (credit card and ATM networks), and could have significant consequences if attacked, but there are also many country- and product-specific systems that are crucial. These include: specific forms of payment systems used to settle financial transactions for products in the equity, bond,

[11] A Zero-day vulnerability is an undisclosed computer-software vulnerability that hackers can exploit to adversely affect computer programs, data, additional computers or a network.

[12] OFR "Cybersecurity and Financial Stability: Risk and Resilience". February 15, 2017.

[13] Cap Gemini and BNP Paribas "World Payments Report 2016."

currency, futures, derivatives and options markets, and to transfer funds between financial institutions both domestically using clearing and real-time gross settlement (RTGS) systems (like TARGET2 in Europe or Fedwire in the US), and internationally using the SWIFT network.

With this background, one scenario could see a big wholesale payment system and a large retail payment system attacked at the same time, so that neither can provide their services, for example, over a 24-hour period.

Many Financial Market Infrastructures (FMI) already have some of the most resilient systems and procedures in place. Guidance on cyber resilience by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) also encourage FMIs to preempt attacks, to respond rapidly and effectively, and to achieve faster and safer recovery objectives if the attacks succeed. The Guidance also provides authorities with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber-risk.[14]

In the hypothetical case that such an FMI is disrupted, it could lead to uncertainty about whether FMIs will be able to deliver finality of settlements of obligations related to payments due by the end of that day. This is especially important since many credit, market and legal risks are allocated through complex chains of participants in payments transactions based on the principle of finality. That means that there can be knock-on effects on all parties involved if finality cannot be achieved in a settlement system or if entitlements based on transactions that are legally final cannot be tracked through the system.

From a general point of view, the following impacts could be expected in the described scenario:

- In general, all cross-border and domestic transactions between banks operating through the attacked large-value payment system might not be settled. This could lead to liquidity issues for receiving parties, breach of contracts, failures of payment or delivery obligations, etc.;
- Payments from the attacked large-value payment system's users to CCPs might not be settled[15]. If no initial margin were to be received, it would postpone the start of trading in the respective market or, if some margin were not paid, the positions of the concerned members might be closed out and the members would be in default and might eventually be excluded. Additionally, if there is a large payment shortfall by its members, the CCP itself might have problems in satisfying its payment obligations and could potentially fail;
- Payments from the attacked large-value payment system's users to other FMIs would not be settled, with similar consequences to the two cases above;
- All transactions involving at one stage or another the attacked retail payment system would not be possible, including withdrawing money from ATMs or using cards at merchants or for e-commerce;
- All these impacts above could also create a lack of confidence in the system that could trigger bank runs, which would exacerbate potential liquidity issues that some banks might be already facing, or even cause the failure of some of them;
- A direct impact on the stock and derivatives markets could be expected, affecting the liquidity and prices of financial instruments heavily; and,
- The recovery from such a long disruption in the service would not be easy, and given that complexity a significant number of legal cases could follow.

Scenario 2: Integrity of data

In the modern, digital financial system data binds everything together. As such, all financial sector participants would include data as one of their critical assets within their cyber-strategy.

Data should be readily available to use, but at the same time as the principle of availability, it should also follow the

[14] CPMI-IOSCO "Guidance on cyber resilience for financial market infrastructures." June 2016.

[15] A CCP has the potential to reduce significantly risks to market participants by imposing more robust risk controls on all participants and, in many cases, by achieving multilateral netting of trades. It also enhances the liquidity of the markets it serves, reducing risks to participants. A CCP margin call is a demand by the CCP to a clearing member for additional funds or collateral to offset position losses in a margin account.

principles of confidentiality and integrity, all of which are essential for the correct functioning of the financial system. A cyber-attack could threaten all or some of those principles, and could consist of:

- Leakage of data
- Loss of data
- Compromised integrity of data

The theft of data from an institution could be for intelligence gathering, or getting personal and confidential information about clients that could then be sold or used for further cyber-attacks (using passwords of clients, getting credit under their names, etc.) These attacks can go unnoticed for a long period and when discovered, they can create confidence issues and economic losses, but it is unlikely that they pose a threat to financial stability.

However, if the attack consists of a ransomware attack involving encryption of data or corruption of the integrity of data, the consequences could be far reaching. One of the hypothetical scenarios under which such an attack could threaten financial stability is major data corruption at a custodian bank and one of the large Central Securities Depositories. To better understand this scenario, below is a description of the role of these types of institutions.

A primary role of a custodian is to act as an intermediary between an institutional client that invests in securities and other investment assets and the Financial Market Infrastructures that clear and settle transactions.

It could be said that the main risk of a custodian bank is operational risk, given the vast amount of data it relies upon every day. It is important to clarify that the official records of securities transfers are maintained by Central Securities Depositories (CSDs) and International Central Securities Depositories (ICSDs). Custodians manage, report and track changes in ownership through CSDs and ICSDs in securities holdings on behalf of their clients. For this reason, the following scenario also includes an attack on one large ICSD (but the same issues could arise with a domestic CSD).

The services provided by the largest custodian banks and the ICSDs are critical to the normal functioning of the financial system. As detailed before, the clearing, settlement and safekeeping of securities is a multi-tiered system, so there are redundancies in place that make it stronger. For example, there is a reconciliation process that ensures that positions held by CSDs or ICSDs are the same as the ones recorded by custodian banks. If one institution's data were attacked, the correct and complete data could be reconstructed.

But any successful attack on the integrity of the data of all these institutions at the same time would pose a real threat to financial stability as, at least, the common operations between the attacked custodian banks and the ICSD would be difficult to reconcile or reconstruct, especially in the short time that markets would demand. The main consequences could be:

- Purchases and sales of the securities involved might not all be processed;
- The critical service of providing safekeeping and record keeping of securities for clients might be compromised, at least for a period;
- The price of the affected securities could be altered or skewed and this could result in a trading disruption;
- More complex operations carried out by custodians and ICSDs, such as securities lending might be affected; and,
- Reputational damage may trigger a wider loss of confidence.

Scenario 3: Failure of wider infrastructure

Direct attacks on parts of the wider infrastructure that the financial system relies upon could also result in financial stability implications. This includes attacks on utilities such as transport, telecoms, cable companies, and technology companies, including providers of data storage or cloud computing and other services.

Mark Carney, the Governor of the Bank of England and Chair of the Financial Stability Board, warned in January 2017 that Fintech materially impacts operational and cyber-risk. "Regulators need to be alert to new single point of failure risks such as if banks come to rely on common hosts of online banking or providers of cloud computing services"[16]. It could be said that when these single points of failure are identified, fallback plans should be evaluated.

[16] Mark Carney "The Promise of Fintech – Something New Under the Sun?" Jan. 25, 2017.

This scenario focuses on electricity utilities that provide much of the energy underpinning modern society. As such, the reliability of the electric system is a key national security concern of all countries. While advancements in energy grid technology have allowed for a more dynamic, reliable and efficient system to provide energy, the U.S. Department of Energy notes in its "Quadrennial Energy Review" that this has also simultaneously resulted in greater integration of existing networks, which impacts security. "A power outage caused by a successful future cyberattack could undermine "critical defense infrastructure," damage the economy and place at risk the safety of U.S. citizens." [17]

The same report goes further to say that "Cyber threats to the electricity system are increasing in sophistication, magnitude, and frequency. The current cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities, juxtaposed against the slower-moving deployment of defense measures."

The costs of blackouts alone could be enormous. Allianz estimates that even short blackouts that happen several times per year in the US add up to an annual estimated loss of between USD 104 billion and USD 164 billion.[18]

Such attacks are more likely to belong to the "cyber-war" category such as, according to Ukrainian investigators, the disruption in December 2016 of a Ukrainian power substation that left part of Kiev and its surroundings without electricity for almost 75 minutes.[19]

Most large financial institutions have energy capabilities in place, including back-up supply, to ensure business continuity. But an attack on multiple power grids, including across borders, could overwhelm the defenses supported by individual institutions which are generally designed to generate power only for limited periods.

The consequences would depend on the extent of an attack and its duration, but especially important is the impact on real-time operations flowing through the affected financial institutions and broader market and payment systems, as flows could be significantly delayed or stopped.

Scenario 4: Loss of confidence

When cyber-related events seriously impact the financial system, it invariably results in a loss of confidence. Under such scenarios, retail consumers and broader society could begin to distrust the safety and soundness of parts of the financial system. This could happen both because of a few very significant cyber-attacks or many very frequent successful smaller attacks on financial institutions or on financial markets infrastructures.

Such a broad loss of confidence could materialize in a reduced volume of operations, increased volatility in market prices of financial instruments, hyperinflation, stock market crashes, extensive cash withdrawals from clients, reduced capital flows and a disruption in international trade. It can be expected that institutional investors would take a more measured approach than retail investors when overall confidence in the system is tested.

Even smaller cyber-attacks, because of the diversity in types, number and increased frequency (thefts of client data, theft of money from client accounts, denial of services, etc.), could contribute to a sense of uneasiness and a general loss of confidence in people and companies alike.

Those types of scenarios would certainly impact economic growth in the affected countries, and most likely beyond, and could weigh heavily on the functioning of the financial system.

MEASURES IN PLACE

The financial sector has long been the leading target for cybercriminals and as such financial institutions have invested significant time, money, and resources to anticipate, detect and stop or mitigate cyber-attacks. Given the value of not only the money held at institutions but also the data, the financial sector as compared to other sectors has relatively more sophisticated IT and control systems. Risk management departments in financial institutions may also quantify and provision for cyber risks through Cyber Risk Insurance.

Management boards, Chief Technology Risk Officers and Chief Information Security Officers (CISO's) view cyber-

[17] US Department of Energy "Quadrennial Energy Review." January 2017.
[18] See http://www.agcs.allianz.com/insights/expert-risk-articles/energy-risks/.
[19] See Infosecurity Magazine: "Ukraine Power Outage Confirmed as Cyber Attack", January 12, 2017.

resilience holistically across their firms. The concept of cyber resilience provides a holistic approach to protecting against cyber-attacks. Rather than simply focusing only on prevention, cyber resilience also focuses on corrective actions, such as having solutions in place to continue business operations should an attack occur. Cyber resilience ultimately refers to the preparations that an organization makes in regard to preventing threats and vulnerabilities (the defenses that have been developed and deployed), the responsive actions available for mitigating a security failure once it occurs, and its post-incident recovery capabilities.

There are also a number of information-sharing platforms in place (such as the aforementioned FS-ISAC initiatives), and others in development, that encourage financial institutions, in cooperation with authorities, to share intelligence on attacks, including real-time incident reporting. However, information sharing has its challenges, which must be carefully assessed and addressed.[20]

Authorities are also increasingly developing approaches to cyber-security, which encourage firms to assess security vulnerabilities relating to people, processes, and technology to better protect themselves, including through simulation exercises and penetration testing[21]. Policy-makers are also introducing a variety of measures around the world aimed at boosting cyber-resilience, such as the ones addressing the growing concern about the wider infrastructure and reliance on third parties by requiring cyber-due diligence of these partners across the supply chain. Given the substantial differences in regulations currently being introduced, this could lead to regulatory fragmentation, which can lead to duplication or even inconsistencies or conflicts for internationally-active firms.

As such, it is welcomed that the G20 has called upon the Financial Stability Board (FSB) to undertake a "stock-take" of existing cyber security regulation as a basis for developing recommended practices in the medium term.[22] The FSB has committed to producing a report to the G20 by October 2017.

GOING FORWARD

While both the private sector and the authorities have done much to address the increasing threats arising from cyber-attacks, more analysis needs to be done of the emerging threats to financial stability. This could include the industry collaborating more closely with the regulatory community to offer lessons-learned advice and expertise on effective cyber practices and assessments.

Public-private collaboration could also be encouraged and further developed, given the shared interest among both the public sector and industry in finding solutions, removing impediments to sharing information, and building resilience across the financial system.

To contribute building that cyber-resilience, it is especially important to develop and promote a globally accepted cyber-related regulatory landscape that help address the increasing concern of the observed regulatory fragmentation that stems from different jurisdictions issuing cyber-related regulations that are not consistent or even conflict with each other. Fragmentation adds complexity and diverts resources away from security-related activities toward compliance efforts especially for firms that operate in multiple jurisdictions.

Cyber-attacks are increasing and growing in scale, as underscored by the recent WannaCrypt and Petya attacks. While the financial system was relatively spared in these attacks, they are important reminders that the public and private sectors would benefit from working together, to plan for and cooperate to prevent the types of risks.

Collaboration and information sharing among the private and public sector are essential. Whereas progress is already happening in key jurisdictions[23], more can be done internationally to thwart global attacks. Vulnerabilities of the system should be addressed as soon as possible, and it

[20] It is noteworthy that similar issues arising from impediments to information exchange are being encountered in other areas, notably AML/CFT, anti-fraud action, tax, and Over the Counter "(OTC") derivatives reform. As a result, it may be useful for the FSB to coordinate with other work streams in the official sector to make sure data-sharing issues are addressed consistently and without stove-piping that would produce incomplete or inconsistent relief for different purposes.

[21] But there is a need to use a common standard, as for example CBEST in UK. So far supervisors are asking for this kind of practice and many banks end up using different types of penetration testing.

[22] FSB website; and Mark Carney, "Building the Infrastructure to Realize Fintech's Promise," speech at the International Fintech Conference 2017, London, April 12, 2017.

[23] Reuters, May 13, 2017: "G7 nations to agree joint fight against cyber-attacks: draft."

takes deep and constant communication among all parties to accelerate that work as much as possible. Where there are regulatory hurdles to information sharing, these should be addressed and platforms should be created that can help remove the limitations on data sharing. A good example is the European Parliament resolution on Fin Tech[24], where the Parliamentarians highlight the need for exchange of information and best practices between supervisors, as well as regulators and governments at their respective levels.

The following ideas could be considered to improve and enhance information sharing:

- One-stop-shop mechanisms, so that any given firm reports incidents only to one "home" or "leading" supervisor or authority, which will then coordinate with other supervisors and authorities;
- Two-way information sharing, so not only companies report incidents to supervisors or authorities, but information also flows in the other direction, alerting companies to emerging issues, threats, or counter-threat measures as soon as possible;
- Further promotion of incident-sharing networks among financial institutions (which also requires addressing information-sharing impediments);
- Ensure quick information sharing processes that match the speed at which cyber-criminals work; and,
- Develop mechanisms for effective cross-sectoral exchange of information.

Additionally, law-enforcement bodies in charge of policing cyber-attacks could be given additional legal tools to stop attacks and minimize the damage. For example, there could be closer international agreements to expedite extradition of hackers, impose penalties on non-cooperative countries or cyber-havens. There could also be measures in place to avoid crashes or contagion effects, etc. Better coordinated enforcement would disrupt the cost-benefit that encourages profit-seeking cyber-criminals, therefore reducing the likelihood of attacks.

Other initiatives are also relevant, such as improving detecting capabilities by relying on new technologies such as Big Data and Artificial Intelligence to detect weak signals and anticipate issues, or active threat hunting that allows organizations to hunt, disrupt and deter attackers in a form of offensive (vs. defensive) cyber-posture.

Obstacles to financial institutions' sharing information among themselves and with law-enforcement and regulatory authorities in all relevant countries should be closely analyzed.[25]

Periodic crisis management exercises involving the financial industry and critical infrastructure institutions are also an effective way to identify potential shortcomings and increase preparedness for attacks with systemic consequences.

The public sector could consider increasing the public awareness of cyber-risks to the financial system. Good training programs for businesses and awareness campaigns for the public, and orienting the educational system to train more cyber-experts could help make the financial system more resilient.

Finally, to address the risk of loss of confidence across wider society, the authorities could oversee the coordination of communication initiatives (from the public and private institutions involved), so that if such an event where to happen, the public in general would be well informed and aware of the rights and responsibilities of institutions and individuals, and, to the extent possible, remedial measures being taken, thereby helping to reduce uncertainty or panic.

In summary, cyber-resilience of the financial system must be approached holistically considering all the actors involved, using the many technical and legal tools available, developing new ones if needed, and always seeking international cooperation and promoting harmonization. Cyber-attacks do not stop at the border, and neither should the efforts aimed at responding to them.

[24] European Parliament resolution of 17 May 2017 on "Fin Tech: the influence of technology on the future of the financial sector."

[25] Obstacles to effective cross-border and domestic exchange of information include, inter alia, inconsistent legal frameworks for data protection, privacy, suspicious transaction reporting and bank secrecy across different jurisdictions along with the regulatory and legal barriers incumbent therein.