CYBER-SECURITY AND CYBER-RESILIENCE

1. Current industry practices and trends

1.1. Evolution of cyber-threats and risks

An industry representative explained that their company, an insurance firm, views the evolution of cyber risk through 20 years of cyber claim data and assessment of risks inside portfolios. Financial institutions have historically been the main target of cyberattacks, but as these companies have increased the robustness of their defences there has been a shift in attacks to other sectors. All financial institutions are likely to face at some point some form of cyber-attack. In 2018 the frequency of cyber-attacks grew with more cyber claims reported than in the previous two years combined. In addition, there has been a shift in the methods that cyber criminals use and also in the geographies targeted. In 2018 the three main methods used were business email compromise[1], ransomware and data breach.

Another industry representative stated that what most concerns them is the development of massive, well structured attacks such as WannaCry and Carbanak from large scale criminal organisations which go beyond the protection and measures that individual companies and banks can put in place. Regarding Carbanak for example, a few years ago, there was an enormous attack lasting two years from a large scale organisation across 30 countries. 130 banks were hit and the total loss was around €1 billion.

A third industry representative added that cyber-risk is a global problem with national implications. Effects in different parts of the world have the ability to create operational shocks in other countries, so it is a borderless issue. Considering market infrastructures for example, it is important to be able to respond to these potential cross-border impacts. Another characteristic of cyber risks is that they are intentional, unlike other operational risks.

An official summarised that cyber risks are on the rise and are changing rapidly. Risks are not idiosyncratic; they are pervasive and multifaceted, and as a result of the nature of the financial system they are cross border and system wide, specifically from a financial stability perspective. Attacks are becoming increasingly sophisticated and some are harming the financial system, as well as economic and political stability.

1.2. Main underlying factors of cyber-risks and challenges for the financial sector

An industry representative stated that there are several trends underlying cyber-attacks. The first is usually human error with employees or other individuals unintentionally opening the door to criminals or cyberattacks. The second is how companies respond after an attack. Having a robust response in the first 48 hours is critical as it helps to limit the size of the attack and its potential loss but also helps companies to get up and running much more quickly. This entails having a robust crisis management plan and bringing in the right forensic data experts and potentially public relations in order to mitigate reputational impacts and customer loss risks. Investment in response and recovery capacities after a cyber-attack are as important as the identification, protection and detection of cyber-risk prior to it.

Another industry representative felt that there are three primary sources of threat to the financial services sector. The first comes from increased criminal activity, whether from organised cyber-criminals or nation states. There has been an increase in the amount of cyber activity coming from those groups. The second is the increasing use of new technologies[2] in service offerings, which creates several challenges including the difficulty of understanding the gaps created when integrating new and old technology and the need to integrate technology quickly due to competitive pressure without fully understanding the risks and implications. And third, the growing outsourcing to fintechs and other third parties, which increases the potential surface and entry points for cyber-attacks.

These threats are exacerbated by the interconnectedness within the financial services sector and the complexity of financial markets, which makes cyber-risk a systemic issue. Cyber resilience indeed involves understanding how a product or service is accomplished from origination to delivery to the market and the underlying practices and disciplines. This requires qualified resources that are scarce.

A third industry representative agreed that increasing digitalisation and outsourcing (e.g. to cloud service providers) make cyber-resilience increasingly difficult. It is very difficult in particular to implement the specific requirements needed by individual financial institutions when dealing with global cloud service providers.

An official concurred with the different drivers of cyber-risk mentioned by the industry speakers, emphasizing that time to market pressure, which has increased with digitalisation and competition is pushing firms to move into new fields without always the adequate preparation for and protection against cyber risks. Another official noted that time to market pressure is relevant for example in the area of payments with developments related to instant payments tending to go as fast as possible.

1.3. Cyber-resilience and cyber-security actions undertaken by the financial industry

Speakers believed that progress is generally being made with considerable investments by financial institutions, although there is still room for improvement.

An industry representative suggested that three main steps are necessary to mitigate cyber-risk: realising the magnitude of a problem; investing in procedures to address cyber-risks; and taking the attackers' point of view. There is now a realisation of the magnitude of the threat in the financial sector and there is investment underway in framework practices. In addition ethical hacking exercises and bug bounty platforms[3] are used by many institutions to identify and tackle cyber-vulnerabilities.

A member of the audience was concerned by some industry players who still believe that cyber-risk can be tackled by taking an insurance or putting capital aside to fight a cyber-attack. An industry representative agreed that insurance is not the panacea to all cyber threats. Insurance companies help financial institutions to analyse their risks and cover some of them but they cannot insure all the cyber risks of a company, so it is definitely up to financial institutions to invest in their defences and employee training. Although there has generally been great progress within financial services in fighting cyber-risk, there is some bifurcation between larger corporations

that have more resources available and smaller and medium sized companies. The smaller ones are sometimes not able to deploy the same network defences and information security sensors, so might rely on external vendors to increase the robustness of their defences, creating potential vulnerabilities.

2. Main areas of improvement in the financial services sector

2.1. Areas of improvement at an individual company level

An official believed that self discipline could be reinforced, particularly regarding cyber governance. In some cases, cyber strategy is still non existent or not operationalised and it is often not included in the global risk management strategy of financial institutions.

In addition, there is a need for the industry to adapt its cyber security approach and widen its scope from detection and protection to the ability to respond in the case of an attack. Scarcity of resources is a challenge in this perspective. Given the complexity of the financial sector, there is a need to set priorities on where and how to use these scarce resources. It is also essential to have a cross-jurisdictional and cross-sectoral coordinated action to address these challenges, which should involve both the financial industry, public authorities, security agencies and potentially other industry sectors concerned by cyberattacks.

Another official stressed that the industry should also consider expanding its thinking and actions beyond cyber risks to cover hybrid threats, which involves using broader risk scenarios in particular. This is one of the priorities of the Finnish EU Presidency.

2.2. Progress needed at sector level and information sharing

A public representative summarised that attacks are on the rise and have a potential systemic nature, so no organisations can defend themselves alone. A global, systemic and more organised line of defence is needed involving industry players and also supervisors, both at a global and European level. Information-sharing is also part of this.

An industry representative believed that firms need to understand how to be resilient to cyber-attacks throughout the whole supply chain, including third parties. Firms also need to work together as a sector to ensure cyber-resilience, considering the different intermediaries and suppliers used to deliver a given product or service, the current controls in place to manage cyber risks, and how the industry will respond if the risk materializes.

Another industry representative stated that in facing these threats a first step for companies is to strengthen their individual continuity plans and develop additional cyber resilience action plans. Training and change management can also help to reduce risks of human error. However, given the scale of organised criminal threat that financial institutions are facing individual company action is insufficient. It is also essential to increase the number, breadth and innovation of simulations in order to address the new challenges raised notably by digitalisation. Sector or industry level exercises, such as the one the G7 ran last June are a good example of this. Work is also underway at the industry-level to introduce new approaches. For example, several industry players are using cyber red teaming[4] to continuously test the vulnerability of the systems, instead of testing one given point.

An official explained that areas where the industry could work together have been identified and industry-led working groups are active in three main areas: data integrity (e.g. regarding how asset ownership can be recovered following an attack on a CSD), information sharing, and the verification of the level of security of third-party providers.. Constructive feedback has also been received from the industry regarding guidance defined by the BIS, especially on the two hour recovery time objective.

A member of the audience noted that some companies already have several years' experience in collecting operational risk data in the financial sector, including on cyber security risk, and that exchange of information about events is a well-rooted practice that should be used.

An official emphasized that although data collection is already happening, some issues remain to be tackled. Some of the data remains confidential. There are also consistency issues that require defining a common vocabulary and methodology for measuring the impact of incidents. This would help to qualify them better and in a more comparable way. An industry representative agreed that confidentiality issues are an obstacle to information sharing. If there was a reporting requirement to a regulatory body that would help to get a more complete information on cyber-breaches.

2.3. Improvement of the management of outsourcing arrangements

Outsourcing arrangements were mentioned as a potential driver of cyber-risk by several speakers.

An official emphasized that while it is right to outsource tasks, responsibility cannot be outsourced. One source of improvement would be for the industry to collaborate in the assessment of third-party providers and in the determination of those who are secure enough from a cyber-security perspective.

Another official felt that it is also important to check whether responsibilities are appropriately defined and that cyber security is being well handled by the service provider. The outsourcer also needs to be in a position to control risks posed by third parties. For example, it can be difficult for single financial institutions to oblige the very large cloud service providers to change their practices. Using safe contractual and functional arrangements is also essential to tackle the risks related to outsourcing, especially between market infrastructures and their providers.

A public representative agreed that the ability of the outsourcer to control risks and therefore to exert its responsibilities is an issue when financial institutions outsource to a larger company, which is often the case. A separate issue is when all financial institutions outsource to the same small group of companies. The concentration of services outsourced to a small number of providers poses financial stability risks and raises questions about how to control them. Control needs to be cross jurisdictional and cross sectoral and also requires a great deal of resources, which is challenging to put in place.

An industry representative suggested that the need for a regulation and supervision of third parties could also be considered in order to achieve resilience across the whole marketplace. A member of the audience wondered whether large global providers such as cloud service providers, who play a structural role for many institutions are open to scrutiny by the supervisors or by the industry regarding cyber-risks in particular. A public representative expected companies that provide outsourced services to be open to more scrutiny, especially those in very concentrated sectors. It is in their interest to be open to this type of assessment in order to mitigate the potential systemic risks this situation may pose.

3. Ongoing public sector initiatives at the EU and global levels

3.1. EU regulatory and supervisory approach to cyber-resilience

An official stated that attempts to promote cyber security have been taken by the public authorities, which have led to a number of initiatives globally, at the EU level and also nationally. The EU Fintech action plan proposed in March 2018 requests that the European supervisory authorities (ESAs) should provide the Commission with technical advice on how to develop a coherent cyber resilience testing framework and evaluate the related costs and benefits. Subsequently two pieces of joint-advice were published in April 2019[5].

The first one relates to legislative improvements. Several potential regulatory actions that could be taken have been identified including minimum requirements for ICT risk, security management at financial sector companies, the harmonisation of ICT incident reporting, the outsourcing of critical services and an appropriate oversight framework for monitoring the activities of third party providers.

The second piece of advice relates to the costs and benefits of developing a coherent cyber resilience testing framework. The ESAs concluded that red team testing is one tool in a broader toolkit for achieving cyber resilience, but on its own it is insufficient and requires a certain level of cyber maturity of the entities being tested. The authorities have also recognised that cyber risks are typically managed as part of financial institutions' traditional operational risk management framework, which is not sufficient.

The actions of the EU and ESAs are steps in the right direction but the official believed that further progress is needed, notably to tackle the mismatch between strong financial integration and limited security integration. The supervisory infrastructure has become more centralised, particularly with the Single Supervisory Mechanism and the ESAs, but there is no corresponding coordination of institutional collaboration at an industry-level. Improving information sharing and enhanced cooperation between the public authorities and the private sector is essential.

An industry representative also noted that the fragmentation of current rulemaking can be an obstacle to the improvement of cyber-resilience at the sector level. This would require the cross-border and cross-sectoral dimensions of cyber-resilience to be better taken into account by the public authorities in the regulation and supervision of financial services.

An official considered that at the EU level, the ESAs and the euro area authorities should consider holding cross border preparedness exercises regularly. The Nordic region is an example of cross border cooperation, as its banks are heavily interconnected, have similar funding structures and are exposed to similar risks. As part of that cooperation the Nordic countries have started to implement the TIBER-EU red team testing framework in a coordinated way. Cooperation in other areas, such as threat intelligence sharing and the consolidation of legal frameworks, should be the next steps. Going forward other industries need to be brought in as well, as it is not just a financial sector issue. An audience member noted that when annual crisis management exercises are conducted annually by the Dutch Central Bank in the Netherlands in the context of TIBER testing, the telecom and energy industries are included. The next step is to perform cyber resilience and operational resilience jointly, with a TIBER framework that is broader than just the financial sector.

3.2. Initiatives and cooperation at the global level

An official stated that at the global level cyberattacks are now considered one of the major risks facing the financial sector. Cyber resilience was a building block of the mandate of the G7 French Presidency and G7 jurisdictions agreed to deepen their engagement on this issue in three specific areas: (i) regulation while maintaining a balance with self-discipline at the industry level; (ii) information sharing with an improvement of the harmonisation and categorisation of incidents; and (iii) crisis management with the decision to conduct cross-border crisis management exercises at the G7 level[6].

Answering a question from the Chair about the possible need for additional guidance at the international level regarding cyber-resilience and information sharing, another official did not think that was necessary. Sufficient guidance already exists such as the one established by CPMI IOSCO and the industry now needs to cooperate in the implementation of those guidelines. This guidance is about protecting the core of the financial system, but CPMI is also working on securing the periphery with a strategy on how to secure endpoints in the payment system, particularly wholesale. Later this year CPMI will develop and publish an implementation toolkit for this strategy.

Answering a question about how to operationalise threat-sharing at the global level, an industry representative explained that it depends on the type of information concerned. Companies can share best practice information, but other types of threat information may have national security implications, which are much harder to share, especially across jurisdictions. There are also issues of trust and indemnification.

---

[1] In a business email compromise attack, what typically happens is that criminals use credible looking spoof accounts to impersonate executives or potentially a crucial supplier or vendor to the company. They target employees who are authorised to transfer money or other valuable data. Those types of attacks can be greatly exacerbated by the use of embedded malware spreading things across the whole corporation. In the ransomware world, attacks have become increasingly targeted and malicious, leading to longer downtimes and more difficulty recovering data or restoring it from backups.

[2] With the development of artificial intelligence, machine learning, robotics and distributed ledger.

[3] A bug bounty program is a deal offered by organizations, websites and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to vulnerabilities.

[4] Cyber red teaming is the practice of using a team of experienced cyber individuals with knowledge of the techniques, tactics, and procedures of an adversary to test the plans, procedures, and responses of an organization in order to improve the organization's cyber posture.

[5] Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements in the European Union (EU) financial sector. Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector.

[6] A first exercise was conducted involving G7 financial authorities and the private sectors from France, Italy, Germany and Japan. The objective of the exercise was to enhance coordination among G7 financial authorities in responding to cyber incidents. The test was intended to cover certain questions. The first question was whether counterparts were able to communicate amongst themselves and exchange information, both inside the country and across borders, in a timely manner. The second question was whether counterparts could correctly assess the situation and collect relevant data to manage the crisis, and whether they had the appropriate mechanisms for a coordinated and timely response and recovery. The third question was how to communicate decisions in a coordinated manner and response to all stakeholders. Following this the G7 jurisdictions agreed to establish a programme of exercises in the coming years in order to improve operational procedures for response and recovery.