Cyber-security and cyber-resilience

Morten Bech

Head of Secretariat, Committee on Payments and Market Infrastructures (CPMI), Bank for International Settlements (BIS)

Cyber-risk requires an innovative implementation of global standards

Good delivery gold bars worth $81 million would weigh as much as an adult hippopotamus. Yet the criminals who looted an equivalent value of funds from the Bangladesh Bank's account in New York in 2016 never needed to break into a sweat. Instead, they moved the stolen money with a few mouse clicks.

Technology has vastly improved access to financial services, to say nothing of their quality and convenience. At the same time, of course, malefactors have turned these advantages to their own nefarious purposes.

The CPMI's response to the Bangladesh Bank heist was a strategy published last year: Reducing the risk of wholesale payments fraud related to endpoint security. This followed the CPMI's and IOSCO's Guidance on cyber resilience for financial market infrastructures, which led the way for standard setters in this field. Most bank supervisors use this guidance too, as confirmed by the Basel Committee on Banking Supervision in their report on Cyber-resilience: Range of practices in December 2018.

> *"To meet the challenge posed by cyber risk, new ways of collaborating with the financial industry are being explored ..."*
>
> - MORTEN BECH

Central banks and standard setters are now innovating to implement these recommendations. For example, CPMI-IOSCO have set up industry-led working groups to cooperatively investigate solutions to common issues (such as data integrity, information-sharing and risks from third-party service providers). But cyber risk cannot be boiled down to a pass or fail test; managing it requires a cooperative approach with all stakeholders working together.

Exploring areas for cooperation highlights the financial system's high degree of interconnectedness. It is precisely this new kind of risk that the CPMI's endpoint >>>

>>> security strategy is designed to address. The strategy is targeted not just at payment systems but takes in the whole ecosystem and its stakeholders.

Even so, many stakeholders are still unsure what they should be aiming for. To help them, the CPMI is working with its members and the wider industry to develop a list of emerging practices. Available by the end of this year, this will be a living document that will be updated as jurisdictions across the world make progress in their joint endeavour.

So criminals and standard setters are both innovating. Criminals focus on the same crimes, yet constantly renew their methods. Standard setters focus on a resilient financial system, while ceaselessly finding new ways to achieve it. To meet the challenge of cyber risk, collaboration with the financial industry is being explored, cooperative partnerships are broadening, and the fruits of these innovations will be shared globally. A global threat must be met with a global response. ●

Nathalie Aufauvre

Director General Financial Stability and Operations, Banque de France

Addressing cyber-risks: shaping the future of global finance

Financial market infrastructures (FMIs), together with banks and other financial institutions, have these past years constantly gained in technological sophistication, allowing for higher efficiency and speediness in the provision of services, while their role in the smooth functioning of a deeply interconnected and global financial system has never been that pivotal. If this trend has its own benefits, the fact that it takes place in a context marked by the rise of cyber threats has led financial authorities to heighten their vigilance over the associated risks, considering not only the FMIs in isolation but also their ecosystem.

In particular, as FMIs' reliance on critical service providers has kept increasing, overseers and standard setters have deemed necessary to develop dedicated approaches, with a view not only to heightening awareness of the resulting operational risk but also to ensuring safe contractual and functional arrangements between market infrastructures and their providers. A number of initiatives are underway to address the contagion risk - which is at stake here - both at European (e. g. launch of a European Cyber Resilience Board) and international levels (within the G7 notably). Furthermore, the most significant providers (those in particular to which systemic FMIs are exposed) have been incentivized to take strong measures to prevent cyber criminality along the chain.

But of course, outsourcing is only one part of the challenges related to cyber risk and the aforementioned steps are part of a broaden set of efforts undertaken consistently with a recent change of paradigm: cyber risk is not a matter of "if" a crisis occurs anymore, but of "when" it will occur and "how" it will be managed. Therefore, an obvious need for international cooperation arises to enhance preparedness and prompt response in case of major cyber incidents.

"An obvious need for international cooperation arises to enhance preparedness and prompt response."

- NATHALIE AUFAUVRE

This is the reason why the G7Ministers of Finance and Central Banks Governors decided in October 2017, first, to create a communication protocol between financial authorities, and then to test the protocol through a large-scale three days-long exercise, simulating the impact of a significant cyber incident on the financial system. This complex undertaking, performed in June 2019, was the first of its kind involving twenty-four financial authorities: ministries of finance, central banks, bank supervisors and market authorities as well as the private sector in France, Italy, Germany and Japan.

The full potential of the exercise will only be delivered when all lessons will be drawn (what worked well and what need to be improved) without complacency. However, it already confirmed how valuable >>>

>>> crisis simulation exercises are in the building of an operational preparatory capacity to respond to the genuine and growing threat to financial stability posed by the increase of cyber risks. G7 Ministers and Central Bank Governors acknowledged that cooperation among public authorities has an important role to play as regards cyber security in the financial sector. They underlined the importance of deepening their engagement in establishing a programme of cyber exercises for the coming years notably.

The development and the maintenance of crisis management frameworks and communication protocols, ready to be immediately activated in the event of a cyber crisis, as well as the regular practice of coordinated crisis management exercises should also be encouraged at a wider scale. As cyber-risks are not restricted to a country's borders, the exercises should take into consideration the multiplicity of stakeholders from the financial sector itself and possibly with utilities (energy, telecommunication).

There will be no efficient and effective answers to cyber risks without any international cooperation among all stakeholders. ●

Jason Harrell

Executive Director and Head of Business and Government Cybersecurity Partnerships, The Depository Trust & Clearing Corporation (DTCC)

Mitigating risk during tech and outsourcing boom

The financial services industry has experienced a rapid acceleration of technological innovation in recent years. The interconnectedness of the global marketplace has simultaneously risen to an unprecedented level. Consequently, firms are exploring the benefits of technologies like blockchain, artificial intelligence and robotics while increasingly relying on third-party vendors to handle some functions. New technology and outsourcing can lead to significant efficiency improvements and reduced operational costs, but those benefits come with a possibility of elevated risk.

Moving certain operational and non-core functions to outsourced providers or using third parties to develop products and services opens the door for external vendors to gain some level of access to the firm and its confidential data. To further complicate matters, the vendors themselves sometimes employ external providers to deliver their services. While this expansion of the supply chain allows firms to minimize costs and provides an opportunity to introduce innovative solutions more rapidly, it also widens the surface area that could be used for a cyberattack against the firm and, due to the interconnectedness of the financial industry, against the sector as a whole.

A firm's ability to swiftly onboard new technology is often perceived as a positive, enabling the deployment of new technological solutions, ultimately leading to client adoption and enhanced client satisfaction. However, a rush to implement new technology introduces potential risks, and so it is vital that firms understand exactly how it is going to be applied and prepare for any potential vulnerabilities that may arise after implementation.

Regulators and standard setting bodies (SSBs) have taken notice of these new risks and are collaborating with the industry to establish best practices to guide how firms should manage these potential operational impacts.

The UK Supervisors, including the UK Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, recently published a discussion paper detailing the Supervisors' view on what would be required to enhance an organization's resiliency and the steps the supervisor could take to support the sector. In the US, the industry has rallied around the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), a collection of cybersecurity best practices and evaluation criteria. Building upon the advancements of NIST, the Financial Services Sector Coordinating Council (FSSCC), which collaborates with government agencies to protect the US infrastructure from cyberattacks, has introduced a new Cybersecurity Profile, a framework that integrates supervisory expectations to help guide financial institutions in demonstrating compliance with cyber risk management requirements.

"Effective defence mechanisms and resiliency plans are achieved by working collaboratively..."

- JASON HARRELL

As an industry-owned critical market infrastructure, DTCC continues to take steps to further enhance cyber and operational resiliency beyond our own operations. We have been involved in numerous industry-wide testing initiatives, support the sharing of threat information and remain focused on helping to improve cyber and operational resilience sector-wide.

Furthermore, we work closely with participants in other critical sectors to help them determine what controls they possess and how they can continue to improve to guard against cyberthreats. Effective defence mechanisms and resiliency plans are achieved by working collaboratively and implementing best practices, ensuring there are robust measures in place capable of both defending against threats and ensuring the resiliency of critical operations across financial market infrastructure. ●

Tony Blanco

Secretary General and Member of the Executive Board, La Banque Postale

Increased international cooperation is crucial to fight cyber criminality

Cybersecurity has become a major concern for companies. And rightly so, considering the cost of cybercrime, now estimated to exceed $600 billion a year.

The financial sector is a primary target for cybercriminals as it daily manages massive flows of private and financial data in a highly interconnected way. Cyber-attacks prevention and detection therefore has become a top priority for financial institutions and their supervisors. Today, every IT risk manager can confirm that "the question is no longer whether the company will be attacked or not, but when". Corporates, employees and citizens are increasingly responsive to cyber risks and willing to improve protection. Company business continuity plans are strengthened and supplemented with specific cyber-resilience sections, and employee training is reinforced.

However, company level actions are not sufficient to address the growing challenges that the financial sector is facing.

The development of both massive (e.g. wannacry) and bank-specific attacks (e.g. Carbanak) has highlighted the increasing sophistication and level of organisation of attackers and the risks at sector and global levels. The development of IA and Big Data creates additional challenges: future cyber-attacks are likely to be conducted using all the potential it offers. Increasing digitalisation and use of outsourcing in the last years also create additional complexities.

Trust in the security of the financial system is a critical asset that must be protected.

In that context, the highly interconnected nature of the financial sector requires increased cooperation between institutions and between states, notably to share best practices. We welcome the EU propositions about the creation of European network of cybersecurity skill centers that will reinforce European cooperation and resilience.

La Banque Postale supports the EU Cybersecurity Act which provides a safe common market for cybersecurity products and services. It adds a new dimension to the 2016 NIS Directive, which ensures a minimum common standard for information networks in the EU, by setting up an incentive framework for cybersecurity certification both for solution and service providers.

As an example, when considering outsourcing, banks need to be fully aware of technical specifications supporting the solution, and often require costly dedicated modifications to meet these requirements. Turnkey solutions (like cloud solutions) offered by worldwide providers could be certified or labelled "cyber resilient" by a European authority, thus ensuring a security standard both for banks and customers.

"Cyber criminality is ever more organised: to fight it, international cooperation is critical."

- TONY BLANCO

Also, in order to offer innovative services, companies need to test quickly and efficiently their security systems. For this purpose, they often call on communities of cyber hacking experts, using "Bug Bounty" platforms to detect weaknesses (as La Banque Postale did to test the resilience of its digital subsidiary Ma French Bank).

As a natural extension of the Cybersecurity Act, we should consider whether to build a European framework for these platforms, providing certifications at the EU level.

Cyber criminality is ever more organised and sophisticated: to fight this global threat, accelerating international cooperation between states and companies is critical. ●