Future-proofing regulation and supervision November 2018

Workshop 6
Cyber-security and operational resilience

Chair: Lyndon Nelson (Deputy Chief Executive of Prudential Regulation Authority and Executive Director of Regulatory Operations & Supervisory Risk Specialists, Bank of England)

Cyber-risk is rising, with potential consequences for financial stability

In March 2017, the G20 Finance Ministers and Central Bank Governors noted that "the malicious use of information and communication technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability".[1] The swift spread of the WannaCry ransomware and the discovery of the theft of personal information affecting over 140 million accounts at Equifax in May the same year exacerbated the sense of urgency in coordinating international efforts to enhance system-wide cyber-resilience.

Although large-scale cyber-attacks in the form of distributed denial of service, data theft, intellectual property loss and cyber-fraud have existed for the past 15 years, their frequency and impact have grown faster than firms' capacity to prevent and recover from them. According to a recent report, cyber-crime costs businesses close to USD 600 billion, up from USD 445 billion in 2014, making it the third global scourge in terms of dollar value after government corruption and narcotics trafficking.[2] While cyber-security issues affect all sectors and geographies, banks arguably make up the favourite target of cyber-attackers. A 2017 survey estimated that a typical financial institution faces an average of 85 targeted cyber-attacks every year, a third of which are successful.[3]

This faster trend can be explained both by the accelerating speed of technological change and the increasingly interconnected ecosystem banks are part of. In addition, banking is a data-driven industry and banks are therefore competing with other actors in data-driven industries in every segment of their value chain. In particular, the key determinants of the competition for customers, in an environment where social media provide instant global platforms, are the time-to-market and the quality of the customer's experience. But the risk is that these desiderata are achieved at the expense of safety and soundness. Banks are adopting automation and integration strategies that see more data stored and processed outside their regulated perimeters while at the same time granting service providers, including fintech entities, access to their environments to perform business and technology processes. This results in an

1 See G20, *Communiqué: G20 Finance Ministers and Central Bank Governors Meeting,* Baden-Baden, Germany, 17–18 March 2017, www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

2 McAfee in partnership with the Center for Strategic and International Studies (CSIS), February 2018, www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf

3 Accenture, *High Performance Security Report 2016*, www.accenture.com/us-en/insight-building-confidence-facing-cybersecurity-conundrum.

attack surface that is accessible from anywhere, and it incentivises cyber-adversaries to step up their efforts.

At a system level, the International Monetary Fund (IMF) points to cyber-threats as a financial stability risk in its October 2017 *Global Financial Stability Report*,[4] and national authorities have started considering cyber-risk as part of their regular financial stability reports.[5] Among the possible transmission channels identified in these reports, financial interconnectedness, operational dependencies and confidence effects are most mentioned, although both institutions and the official sector struggle to find a comparable set of meaningful metrics to quantify and monitor cyber-risk, and assess firms' cyber-resilience.

Q1. What are the specific challenges posed by cyber-risk as opposed to traditional operational risks?

Q2. Is there any particular technological innovation or development in the current ecosystem bearing systemic cyber-security concerns that supervisors should monitor more closely?

The official sector responses to date

In November 2016, cyber-security was discussed at the ICBS as part of a workshop on "improving best practices in banking services". The risks that cyber-attacks might pose to the financial system as a whole were discussed, as were, in particular, the importance of the human element – ranging from the lack of awareness and skills both among Board members and staff to the challenge of recruiting and retaining savvy professionals – beyond the technical aspects of software and hardware maintenance. Two years ago, legislation governing cyber-security and consumer protection was foreseen by many jurisdictions in order to mandate "certain elements of governance and adherence to certain standards around technology".

Less than a year later, cyber-security concerns reached the top of the international regulatory agenda, focusing the attention of most global standard setters, not only in the financial sector. In parallel, banks have been reinforcing and enhancing their capabilities in the light of emerging threats. The FSB published in October 2017 its stocktake of publicly released cyber-security regulations, guidance and supervisory practices both at national and international level. The FSB found that banking is the only sector in financial services for which all FSB jurisdictions have issued at least a regulation, guidance or supervisory practices. And "future plans" for material to be issued "within the year" were reported by three quarters of respondents (both member jurisdictions and international bodies). In addition, the FSB member jurisdictions reported drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies in developing their cyber-security regulatory and supervisory schemes (mainly the joint Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO) Guidance on cyber-resilience for financial market infrastructures issued in June 2016, the US NIST[6] Cybersecurity framework and the ISO 2700 series). Other international initiatives referenced by members included the G7's Fundamental Elements of Cybersecurity for the financial sector[7] and, in the EU, the European Commission's Fintech Action Plan

[4] See IMF, "Global Financial Stability Report," October 2017, www.imf.org/en/Publications/GFSR/Issues/2017/09/27/global-financial-stability-report-october-2017.

[5] For instance, see the recent financial stability reports of Canada, the ECB, India, the Netherlands, South Africa, and the United States Financial Stability Oversight Council and the Office of Financial Research.

[6] NIST stands for National Institute of Standards and Technology.

[7] See the G7's *Fundamental Elements of Cybersecurity for the Financial Sector,* October 2016.

invites the European Supervisory Authorities to consider issuing guidelines to achieve convergence on ICT risk.[8]

On the other hand, although banks and regulators agree that the existing guidance provides a good set of high-level principles that can serve as building blocks for enhancing cyber-security, a common challenge reported by industry stakeholders is the diversion of time and resources spent on "box-ticking", compliance exercises with sometimes redundant or contradictory regulations instead of effectively building up and maintaining their resilience capabilities.[9] From the official sector's perspective, the diversity of national cyber-security institutional setups and the varying maturity of sectoral initiatives also pose a challenge in designing effective policies, in a context where the system is only as strong as its weakest link.

Q3. Are there concrete instances of regulatory fragmentation (geographical, sectoral) where the addition of requirements actually weakens institutions' positions, and what could be done to address these?

From cyber-security to operational resilience

As cyber-attacks have grown in number, sophistication and disruptive impact, maturity levels in the financial sector have increased too. Among the main lessons that currently drive banks' and regulators' activities, a few are listed below:

- **Basic cyber-hygiene issues still underlie the vast majority of successful cyber-attacks**. This means that massive investments in high-end capabilities and technologies do not necessarily guarantee better protection if flaws in patching, access and password management still exist. Cyber-attackers study the systems they target, and test for potential vulnerabilities starting from the most basic features, often with a phishing email to an employee. Firms and authorities need to continuously ensure a basic level of security, awareness and familiarity with IT tools and practices across all people, processes and technology relevant to a firm's operations.
- **A cyber-incident is a matter of "when" rather than "if"**. Threats may come from external as much as internal sources, and undetected breaches or failures may remain hidden for up to several months, meaning that institutions may succumb to a false sense of security that makes them ultimately more vulnerable. Firms may even be the collateral victims of attacks not originally aimed at them (eg the case of Maersk infected by NotPetya), which means they need to prepare for the unexpected and pay attention to what happens in other countries and industries.
- **Cyber-security has both an operational and business impact.** Cyber-security is no longer solely a matter of information and communication technologies and systems. Every function, service and product operated and designed by firms has a specific cyber-risk profile, which in turn has different business impacts. No capital or liquidity measure can guard against the impact of a critical service or function being compromised, causing the disruption or interruption of essential activities. Therefore, not only should the cyber dimension be part of firm's board-level business strategies, it should also be embedded in its day-to-day activities so as to build processes, services and products that are secure by design.

[8] The European Securities and Markets Authority (ESMA), the European Banking Authority (EBA), and the European Insurance and Occupational Pensions Authority (EIOPA), collectively referred to as the "European Supervisory Authorities".

[9] "Regulatory approaches to enhance banks' cyber-security frameworks", *FSI Insights*, no 2, August 2017, www.bis.org/fsi/publ/insights2.pdf.

These observations have led actors in both the private and official sector to approach cyber-risk management from a broader strategic and operational resilience perspective rather than restricting it to a purely technical discipline focusing on security.[10] Taking a holistic view, the cyber dimension can be seen as one important element of operational resilience. Since breaches will inevitably occur regardless of the level of protection, the risk management approach should not only ensure that controls and mitigation mechanisms are in place, but should also address how to respond, recover and learn from any breach. This kind of contingency and continuity planning implies that a firm's systems be mapped according to their criticality, and that a risk appetite be defined for the firm's assets and businesses against relevant metrics. Such an approach also applies to operational disruptions from causes other than a cyber-attack (eg natural catastrophe or failure of a critical third-party service provider).

Basel Committee work on operational resilience

In this context, the Basel Committee on Banking Supervision (BCBS) recognised the merits of approaching operational resilience beyond the purview of operational risk management and minimum capital requirements, and established the Operational Resilience Working Group (ORG) at the beginning of 2018 with the intention of contributing *inter alia* to the international effort related to cyber-risk management.

The ORG's first task has been to identify the range of existing practice in cyber-resilience, and assess gaps and possible policy measures to enhance banks' broader operational resilience going forward. In launching this initiative, the Committee acknowledged the need for the ORG to take due account of the various international and national frameworks already in place or being developed. ORG member participation in the relevant working groups of the CPMI, FSB, regional authorities and the G7 cyber-security initiatives reflects the Committee's emphasis on ensuring close monitoring and international coordination across the financial sector. At the sole BCBS level, principles related to the risk management of "electronic banking"[11] and operational risk[12] were published as early as 2003 and 2011. The Committee has also published, jointly with IOCO and the IAIS in the context of the Joint Forum, an outsourcing guidance for financial services in 2005[13] and high-level principles for business continuity in 2006.[14] Parts of these high-level guidance and principles remain valid and should form the basis for future policy work, while other, outdated or redundant, parts could be streamlined. Broadly, speaking, the bulk of past and current international initiatives address the following topics, which cover the main supervisory concerns regarding operational resilience:

- Governance frameworks, including the roles of the board of directors and chief information security officer;
- Cyber-risk analysis and assessment;
- Information security, including confidentiality;

10 For instance, the Bank of England has issued a discussion paper seeking to "commence a dialogue with the financial services industry on achieving a step change in the operational resilience of firms and FMIs". See "Building the UK financial sector operational resilience", Bank of England, July 2018, www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A.

11 Basel Committee on Banking Supervision, *Risk management principles for electronic banking*, July 2003, www.bis.org/publ/bcbs98.pdf.

12 Basel Committee on Banking Supervision, *Principles for the sound management of operational risk*, June 2011, www.bis.org/publ/bcbs195.pdf.

13 Joint Forum, February 2005, www.bis.org/publ/joint12.pdf.

14 Joint Forum, August 2006, www.bis.org/publ/joint17.pdf.

- Security controls and incident prevention;
- Expertise, training and broader cultural awareness to manage and address risks;
- Monitoring, testing and/or auditing of controls, including through red or purple teaming;
- Incident response and recovery to investigate, manage, contain and recover from incidents;
- Communication and information-sharing with internal and external, public and private stakeholders both across sectors and across borders;
- Outsourcing relationships and broader third-party dependencies: the perimeter of interest to financial sector regulators has expanded, and the greater use of cloud services means that the perimeter is now also shared; and
- Continuous learning to re-evaluate, test and improve resilience on an ongoing basis, including through exercises and public-private cooperation.

As regards the assessment of the range of existing practices, supervisors are sharing their experience and insights in order to provide a more concrete and specific understanding of the main trends, progress and gaps in the pursuit of cyber-resilience in the banking sector. The BCBS is also committed to maintaining a continuous dialogue with a wide array of stakeholders even beyond the banking industry, to help inform its work towards the design of potential policy measures to enhance the broader operational resilience of banks in the years to come.

Q4. What metrics or indicators could be used by banks assessing and comparing operational resilience levels of their third-party service providers, and by supervisors assessing and comparing banks?

Q5. What practices have been found to be effective in developing and implementing a sound operational resilience framework? What are some of the emerging practices in the field?

Q6. How to improve effective information sharing among banks and regulators across sectors and borders?

Q6. What could be the best way to address the "cyber" competencies/skills challenges that face institutions?

Q7. What are the practical challenges related to the interaction with third-party service providers? What are the challenges faced by third parties in adhering to existing banking requirements?

Q8. Are there implementation challenges related to structural or regional differences that would warrant closer examination by the Basel Committee? Where would standardisation bring most benefits?