Box 4

Financial stability vulnerabilities stemming from cyber risks within financial market infrastructures

A convergence of globalisation and digitalisation has created a financial ecosystem and operational network which is increasingly interconnected and interdependent. In this context, computing and digitalisation are becoming increasingly pervasive. Notwithstanding the many benefits this has brought, this convergence has also increased the susceptibility to cyber attacks.[14] There is a trend towards more frequent and severe cyber attacks, and the composition of the attacks is changing amid growing digitalisation, both of which have financial stability implications. In particular, material financial stability risks might stem from individual systemically important firms or from any prospect of excessive financial market volatility.

One key area of financial stability concern regarding cyber attacks is their potential to disrupt financial market infrastructures (FMIs). Indeed, such infrastructures have become increasingly interconnected and interdependent as an operational network with several critical nodes, as well as harbouring large amounts of confidential data. Such attacks could, in this way, seriously undermine confidence and trust in the financial system. On a daily basis, this network delivers financial intermediation between market participants and end-users, whether the transmission of salaries through FMIs or the settlement of central bank/market transactions through a web of payment and settlement systems, clearing houses, settlement banks and custodians. In a recent survey on critical infrastructures, 48% of respondents found it likely that a cyber attack will take down their critical infrastructure[15]; one study has estimated that cyber crime costs the global economy some USD 400 billion in annual losses[16]; and another study reveals that 83% of financial service organisations experience more than 50 network attacks per month and take an average of 98 days to identify an attack.[17]

Over the last decades, there has been a marked increase in both the frequency and severity of cyber attacks. According to a study by PricewaterhouseCoopers, the number of detected cyber attacks increased sharply during 2015, up by 38%.[18] As recently as 15 years ago, cyber attacks were fairly rudimentary and typically the work of “hacktivists”. However, this appears to be changing with increasing interconnectivity, globalisation and what could be termed a commercialisation of cyber crime.

14 See the top 10 global risks listed in Global Risks, World Economic Forum, 2015.

15 McAfee Labs 2016 Threats Predictions report.

16 Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies and McAfee, June 2014.

17 “Risk & Innovation in Cybersecurity Investments”, Ponemon Institute, 2015.

18 The Global State of Information Security Survey 2016, PricewaterhouseCoopers.

Amid this growing volume of cyber attacks, there has been an evolution in the nature and motivations of the threat actors and their levels of sophistication. The actors have changed significantly over recent years. They range from state-sponsored groups, nation-state proxies, terrorist groups and private enterprises/corporations, to cyber criminals, hacktivists, insiders and lone actors. The nature of the agent attacking an organisation will determine both its objectives and its sophistication. This, in turn, will be reflected in the persistence and breadth of the attack (in terms of the type of hacking tools and resources deployed and the time taken to compromise the organisation). The Threat Landscape 2015 report of the European Union Agency for Network and Information Security (ENISA) notes a number of attack types (e.g. advanced persistent threat attacks), each of which is composed of a number of tactics and tools, such as malware, phishing and denial of service.[19]

Alongside the growing volume and changing nature of attacks, there has been an increasing trend towards digitalisation, thereby increasing the cyber attack surface. More users, data, devices, clouds and network traffic will increase the number of potential routes for attacks; and to further complicate matters, much of this technological advancement will be interlinked with existing IT systems within key financial market participants. Within this complex technological web, a proliferation of threats and vulnerabilities is also likely, notably for critical nodes in the financial system such as FMIs.

All in all, the regulatory response amid a growing prevalence of digitalisation in the financial system recognises both the benefits and the potential vulnerabilities. Digital platforms create more efficient, transparent and in many ways complete global markets. This innovation opens up new possibilities for strengthening economic growth, but these developments must flourish within a safe, efficient and robust financial system. Initiatives are under way to ensure adequate monitoring of these risks across all key financial market players.[20] When it comes specifically to FMIs, global regulators have already initiated efforts to tackle cyber risk, for example by developing the CPMI-IOSCO's Guidance on cyber resilience for financial market infrastructures.[21] Taken together, these initiatives should ensure that regulators, overseers and supervisors of FMIs contribute to strong cyber resilience capabilities, enhance sector resilience and information-sharing and, more generally, foster cooperation and coordination on cyber risks among central banks and other relevant authorities.

---

19 ENISA threat landscape: top 15 cyber threats 2015.

20 For banks, the SSM has indeed identified IT and cyber crime risk as a key supervisory priority for 2016.

21 Guidance on cyber resilience for financial market infrastructures, Committee on Payments and Market Infrastructures/Board of the International Organization of Securities Commissions, November 2015.