Chapter 3

CYBER RISK: A GROWING CONCERN FOR MACROFINANCIAL STABILITY

Against a backdrop of growing digitalization, evolving technologies, and rising geopolitical tensions, cyber-related incidents, in particular those with a malicious intent, have become much more frequent over the past two decades, and especially since 2020. Severe incidents at major financial institutions could pose an acute threat to macrofinancial stability through a loss of confidence, the disruption of critical services, and spillovers to other institutions due to technological and financial interconnectedness.

The chapter finds that while cyber incidents have thus far not been systemic, the risk of extreme direct losses—at least as large as $2.5 billion—to firms from such incidents has increased. Moreover, indirect losses from cyber incidents are also significant and tend to be substantially larger than the reported direct losses by firms.

Understanding the factors that contribute to the occurrence or prevention of cyber incidents is crucial for developing robust cybersecurity policies and strategies. The chapter's analysis suggests that digitalization and geopolitical tensions significantly raise the risk of cyber incidents while more developed cyber legislation and better cyber governance at firms could help to mitigate such risk.

The financial sector is highly exposed to cyber risks with nearly one-fifth of all incidents affecting financial firms. High market concentration and low substitutability, especially when considering critical services such as payment services and custody banking, could make cyber incidents on financial firms particularly disruptive and underscore the importance of strengthening cybersecurity and operational resilience. Operations of financial firms often depend on common third-party IT providers, which also raises the risk of common shocks and spillovers.

A severe cyber incident at a financial institution could undermine trust in the financial system and, in extreme cases, lead to market selloffs or runs on banks. Although no significant cyber runs have occurred yet, empirical analysis suggests modest and somewhat persistent deposit outflows from smaller US banks after a cyberattack.

With the global financial system facing significant and growing cyber risks, policy and governance frameworks must keep pace. However, a survey of central banks and supervisory authorities in emerging market and developing economies shows that cybersecurity policy frameworks often remain insufficient.

The cyber resilience of the financial sector should be strengthened by developing an adequate national cybersecurity strategy, appropriate regulatory and supervisory frameworks, a capable cybersecurity workforce, and domestic and international information-sharing arrangements. To allow for more effective monitoring of cyber risks, reporting of cyber incidents should be strengthened. Supervisors should hold board members responsible for managing the cybersecurity of financial firms and promoting a conducive risk culture, cyber hygiene, and cyber training and awareness. To limit potential disruptions from cyber incidents, financial firms should develop and test response and recovery procedures. National authorities should develop effective response protocols and crisis management frameworks.

The IMF actively helps member countries strengthen their cybersecurity frameworks through the Financial Sector Assessment Programs and capacity-building initiatives.