Banks' cyber security – a second generation of regulatory approaches[1]

Executive summary

Cyber resilience continues to be a top priority for the financial services industry and a key area of attention for financial authorities. This is not surprising given that cyber incidents pose a significant threat to the stability of the financial system and the global economy. The financial system performs a number of key activities that support the real economy (eg deposit taking, lending, payments and settlement services). Cyber incidents can disrupt the information and communication technologies that support these activities and can lead to the misuse and abuse of data that such technologies process or store. This is complicated by the fact that the cyber threat landscape keeps evolving and becoming more complex amid continuous digitalisation, increased third-party dependencies and geopolitical tensions. Moreover, the cost of cyber incidents has continuously and significantly increased over the years.

This paper updates Crisanto and Prenio (2017) by revisiting the cyber regulations in the jurisdictions covered in that paper, as well as examining those issued in other jurisdictions. Aside from cyber regulations in Hong Kong SAR, Singapore, the United Kingdom and the United States, which the 2017 paper covered, this paper examines cyber regulations in Australia, Brazil, the European Union, Israel, Kenya, Mexico, Peru, Philippines, Rwanda, Saudi Arabia and South Africa. The jurisdictions were chosen to reflect cyber regulations in both advanced economies (AEs) and emerging market and developing economies (EMDEs). This highlights the fact that since 2017 several jurisdictions – including EMDEs – have put cyber regulations in place.

There remain two predominant approaches to the regulation of banks' cyber resilience: the first leverages existing related regulations and the second involves issuing comprehensive regulations. The first approach takes as a starting point regulations on operational risk, information security etc and add cyber-specific elements to them. Here, cyber risk is viewed as any other risk and thus the general requirements for risk management, as well as the requirements on information security and operational risks, also apply. This approach is more commonly observed in jurisdictions that already have these related regulations firmly established. The second approach seeks to cover all aspects of cybersecurity, from governance arrangements to operational procedures, in one comprehensive regulation. In both approaches, to counter the risks that might result from having too much prescriptiveness in cyber regulations, some regulations combine broad cyber resilience principles with a set of baseline requirements. Regardless of the regulatory approach taken, the proportionality principle is given due consideration in the application of cyber resilience frameworks.

Whether as part of related regulations or separate comprehensive ones, recent cyber security policies have evolved and could be described as "second-generation" cyber regulations. The "first generation" cyber regulations, which were issued mainly in AEs, focused on establishing a cyber risk management approach and controls. Over the last few years, authorities, including those in EMDEs, have issued new or additional cyber regulations. These second-generation regulations have a more embedded "assume breach" mentality and hence are more aligned with operational resilience concepts. As such, they focus on improving cyber resilience and providing financial institutions and authorities with specific tools to achieve this.

[1] Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org) and Jermy Prenio (Jermy.Prenio@bis.org), Bank for International Settlements, Jefferson Umebara Pelegrini (jefferson.pelegrini@bcb.gov.br), Central Bank of Brazil. We are grateful to Kaspar Köchli and Jatin Taneja for research assistance, and to Markus Grimpe and staff at covered authorities for helpful comments. Esther Künzi and Theodora Mapfumo provided valuable administrative support.

The "second-generation" regulations leverage existing policy approaches to provide additional specific guidance to improve cyber resilience. Cyber security strategy, cyber incident reporting, threat intelligence sharing and cyber resilience testing are still the primary focus of the newer regulations. Managing cyber risks that could arise from connections with third-party service providers has become a key element of the "second generation" cyber security framework. Moreover, there are now more specific regulatory requirements on cyber incident response and recovery, as well as on incident reporting and cyber resilience testing frameworks. In addition, regulatory requirements or expectations relating to issues such as cyber resilience metrics and the availability of appropriate cyber security expertise in banks have been introduced in a few jurisdictions.

Authorities in EMDEs tend to be more prescriptive in their cyber regulations. Cyber security strategy, governance arrangements – including roles and responsibilities – and the nature and frequency of cyber resilience testing are some of the areas where EMDE authorities provide prescriptive requirements. This is approach seems to be connected to the need to strengthen the cyber resilience culture across the financial sector, resource constraints and/or the lack of sufficient cyber security expertise in these jurisdictions. Hence, EMDE authorities may see the need to be clearer in their expectations to make sure banks' boards and senior management invest in cyber security and banks' staff know exactly what they need to do.

International work has resulted in a convergence in cyber resilience regulations and expectations in the financial sector, but more could be done in some areas. Work by the G7 Cyber Expert Group (CEG) and the global standard-setting bodies (SSBs) on cyber resilience has facilitated consistency in financial regulatory and supervisory expectations across jurisdictions. This is necessary given the borderless nature of cyber crime and its potential impact on global financial stability. Another area where there might be scope for convergence is the way in which authorities assess the cyber resilience of supervised institutions. This could, for example, include aligning the assessment of adequacy of a firm's cyber security governance, workforce and cyber resilience metrics. Lastly, there might be scope to consider an international framework for critical third-party providers, in particular cloud providers, given the potential cross-border impact of a cyber incident in one of these providers.