FINANCIAL SECTOR ADVISORY CENTRE (FINSAC)

CYBERSECURITY: THE ROLE OF CENTRAL BANK AND BANK SUPERVISORS

A FinSAC Knowledge Brief

Aquiles A. Almansi and Attila Csajbok

WORLD BANK GROUP
Finance & Markets
Financial Sector Advisory Center (FinSAC)

The threat of cyber-attack is universal and increasing. Any system in any sector that is connected to the internet is vulnerable, and the type and scale of cyber-attacks are only likely to increase and become more sophisticated.

The financial sector is a key target. Cyber-attacks can aim to defraud financial institutions or their customers; to extract business or customer information; to destroy data; to cause damage to the system or make it inaccessible; or any combination of these. Unlike many traditional threats to financial institutions, cyber-attacks can be hard to detect. Systems can be penetrated without this being easily discovered. Even central banks are not immune to cyber attacks.

Supervisors need to help guide national and international efforts to address the threat. Given the high risk of contagion, all connected financial institutions must work to safeguard themselves and the network. Internationals standards address operational risk in terms of capitalization and good practices, but they do not explicitly address the need for resilience to promptly detect and effectively respond to cyber-attacks. Banking regulators and supervisors therefore have a key role in maintaining financial sector stability and are well positioned to provide leadership and coordination in cybersecurity to the banking sector.

The US National Institute of Standards and Technology's cybersecurity framework identifies five core functions to better protect against cyber threats.

- **IDENTIFY** internal and external cyber risks
- **PROTECT** organizational systems, assets, and data
- **DETECT** system intrusions, data breaches, and unauthorized access
- **RESPOND** to a potential cybersecurity event
- **RECOVER** from a cybersecurity event by restoring normal operations and services

The threat extends beyond national borders. Given the cross-border interconnectedness of banking systems, successful cyber-attacks in any part of the network have the potential to spread quickly and widely, threatening not only individual organizations but undermining financial stability. The banking sector needs to share knowledge and expertise.

Cybersecurity is a global priority. There is demand for greater international efforts to develop and align global regulations. ITU, a specialized agency of the UN, have developed the Global Cybersecurity Agenda (GCA) as a framework for international cooperation in this area addressing legal measures; technical and procedural measures; organizational structure; capacity building; and international cooperation. They are also involved in helping countries establish National Computer Incident Response Teams (CIRT) to coordinate responses to cyber-attacks

Measures to better address the risk to the banking sector are being developed. International and regional bodies are looking at the case for introducing legislation. In the EU, plans are progressing for a new Network and Information Security Directive

"The cyber threat to banking – A global industry challenge" produced by the BBA (UK banking sector trade association) identifies scope for the enhanced exchange of cyber knowledge and experiences across the banking sector.

which aims to require banks to ensure they are robust enough to resist cyber-attacks and be ready to report serious security breaches to public authorities. A network of Computer Security Incidents Response Teams (CIRTs) are envisaged, set up by each member state to handle incidents and coordinate responses to cross border security incidents. Non-EU countries are encouraged to consider establishing similar teams.

Despite the threat knowing no borders, Cyber security requirements remain a matter for national governments. Supervisors need to satisfy themselves that the banking sector in their jurisdiction is sufficiently robust to be able to identify and appropriately respond to potential attacks. They need to be aware of incidents affecting any IT system within the financial markets infrastructure, including supervised institutions and other organizations holding sensitive client data. Supervisors should require breaches affecting any part of the network to be notified to them, and have measures in place to ensure this information can be passed appropriately to others in the network but without spreading unnecessary panic or alarm.

Supervisors should encourage cybersecurity to be addressed at the highest level within financial institutions. No organization can realistically completely exclude the possibility of cyber-attack. Too often it has been seen as the role of the IT department but handling risk is the responsibility of the board and cyber risk is no exception. A Board approved framework should be delegated to senior management for implementation with managerial responsibility (senior management), internal validation (internal audit), external validation (external auditors) and supervisory follow up.

The British Government have produced guidance for non-executive directors which stresses the importance of board level engagement to identify and protect critical information and data assets. The Conference of State Bank Supervisors "Resource Guide for Bank Executives: Executive Leadership of Cybersecurity" highlights the measures and actions required of Bank leadership.

Supervisors may decide to require financial institutions to submit cyber management plans. These should detail the systems in place to defend against and to detect cyber-attacks. Although the ever changing nature of the cyber threat makes it difficult for plans to be too prescriptive they should outline the response to an online incident and escalation procedures. Cyber management plans might include:

- A comprehensive map of the network including connections to the internet; operating systems and applications in use; and listing users with administration rights;
- How the network is maintained and updated;
- What technical controls and processes are in place to protect the system;
- What measures exist to ensure that staff and others with access to the system understand how to do so safely and can be trusted;
- How the institution assesses and updates the threat;

- Who will manage the response to an attack;
- How a breach will be contained – to what extent can systems and the network be taken offline and what is the potential impact of this;
- Who should be informed of an attack, both within the financial institution and outside, for example the regulator, law enforcement, and others in the network;
- What might the potential impact be on the operation and reputation of the business, how will this be addressed;
- What needs to be done and in what time scale to get the business operating as normal.

Regular testing of different scenarios will help identify weaknesses in cyber management and improve readiness to respond quickly and confidently to an attack. Supervisors could instigate and take part in the tests or, at a minimum, outline expectations for the test and have the opportunity to discuss the results.

Example of good practice: In the UK the regulator has developed a framework "CBEST" which tests systemically important financial institutions using the latest threat intelligence and tailored to the model and operations of individual businesses.

Supervisors can and should be at the center of cybersecurity efforts - coordinating cyber intelligence sharing and encouraging good practice. Supervisors should be seeking to have a clear picture of the cyber resilience across the sector and to have a contingency plan in place for handling a serious attack on a systemically important financial institution, including who should be informed and how. They should work with colleagues regionally to share knowledge and coordinate actions.

The World Bank Financial Sector Advisory Centre (FinSAC) can help banking supervisors in client countries develop their plans or test their systems. FinSAC is working to highlight the risk to financial stability posed by cyber threats. In May 2015, FinSAC organized a regional seminar on financial sector cyber preparedness for its clients in the Europe and Central Asia region. It is encouraging client countries to establish robust plans to improve cybersecurity and can help test responses to cyber-attack as part of Crisis Simulation Exercises. FinSAC is developing Crisis Simulation Exercises specifically focused on cyber security.

You can find more on the FinSAC cyber preparedness seminar at: http://www.worldbank.org/en/events/2015/05/18/cyber-preparedness-seminar