Lesetja Kganyago: Collaboration for building cyber resilience

Address by Mr Lesetja Kganyago, Governor of the South African Reserve Bank, at the Cybersecurity Conference, Johannesburg, 23 August 2016.

* * *

Governor, Deputy Governors, other distinguished guests, ladies and gentlemen

It gives me great pleasure to welcome you all to this cybersecurity conference with the theme of "Collaboration for building cyber resilience". This is the first cybersecurity conference of this kind to be organised and hosted by the South African Reserve Bank (or SARB), which underlines the importance of cybersecurity and cyber resilience to the South African central bank.

As we stand at the dawn of the Fourth Industrial Revolution, developments in information and communication technology (ICT), spurred on by the digital revolution, have brought and will continue to bring about significant and wide-ranging changes to society and the broader economy. These changes are marked by both speed and ubiquity, and therefore have an impact on almost everyone and most firms and business processes, especially in the financial services sector. While most of these advances have been beneficial, the cyber-world also has its dark side. This is where individuals, groups, and organisations use and exploit the advances made in ICT for ulterior motives. In this context, very few individuals and firms are exempt from or are left untouched by the potentially negative consequences of such activities.

Our Constitution, other legislation as well as the Financial Sector Regulation Bill (FSR Bill), currently before Parliament, place tremendous responsibilities on the SARB. The SARB's primary responsibility for monetary policy will soon be augmented by an explicit financial stability mandate, and our responsibility for the regulation and supervision of banks as well as for the oversight of the national payment system will be expanded to include the safety and soundness of insurers, financial conglomerates, and other systemically important financial institutions, as outlined in the FSR Bill.

Like many other central banks, the SARB plays a key role in the regulation and supervision of the domestic financial system. In our scanning of the financial system for potential systemic risks, cyber-threats have been on our radar for a while now.

As new financial products and services emerge from FinTech innovation and affect the market, the SARB will have to consider their implications for the way in which it conducts its oversight functions as well as monetary and macroprudential policy. The SARB has a balanced approach to these technological innovations. It acknowledges the greater efficiencies that ICT advances have brought to the financial services sector. We have also, within our risk management framework – and like many organisations represented here – adopted and embraced technologies that have helped us to execute our mandate more effectively and efficiently. As a central bank, we are open to innovations despite the different opinions of regulators on matters such as crypto-currencies. We are willing to consider the merits and risks of block chain technology and other distributed ledgers.

Not all innovations in this area are, however, benign. The abuse of algorithmic or high-frequency trading can pose problems for the smooth functioning of financial markets. We understand that many financial and other firms – in their drive for greater efficiency and productivity, and for serving their clients more effectively – may have an even bigger stake in leveraging off these innovations and technologies.

Real opportunities in the digital revolution currently underway await not only further application by the private sector, but also greater utilisation by financial regulatory authorities. As innovations bring down costs, significant transformation of the financial intermediation landscape cannot be discounted or dismissed. Leading innovators know how to turn disruption into opportunity. Possibilities for the use of improved technology in ensuring regulatory

compliance abound for both regulators and the industry. Regulators have only started to scratch the surface of the potential uses of, for example, Big Data in regulatory technology – also referred to as "RegTech". Big Data techniques can assist us to understand the state of the economy and "identify trends in systemic risks" more accurately and quickly.[1] Hopefully, this will lead to further enhancements for policymaking and greater precision in supervisory interventions.

The threat landscape and the role of regulatory authorities

With an expanding digital footprint comes a growing threat landscape, providing greater opportunities and increasing entry points or vectors for cyberattacks. Since the unleashing of the first computer worm in 1988 by a 23-year-old Cornell University student, malware has grown exponentially in both volume and sophistication over the last three decades.[2] There are well over 100 000 known computer viruses and the frequency of cyberattacks has increased. Old defences are quickly rendered redundant. As participants in the financial sector, you are aware of the details of the cyberattacks on privately owned banks, insurers, and other financial institutions without one having to list examples of these.

Even central banks are not immune to such attacks. Reported attacks on SWIFT,[3] the financial messaging network that underpins most international money transfers, have the potential to paralyse global trade and finance, albeit for only a short while.

Spare a thought for ordinary citizens, your customers, who, with their limited resources and information asymmetries, are the most vulnerable and often the biggest losers in attacks where illicit financial gain is the key motive. Innovations, such as the advances in biometrics and digital identities, hold great promise for individual security. We wait for industry to translate these gains into suitable security measures applicable to corporations.

Innovation, however, cuts both ways. Advances in, for example, cryptography prompt further improvement in decryption technology. We therefore cannot be complacent about our cyber-defences.

Given this threat landscape, it is no surprise that cybersecurity has in the recent past moved swiftly up the list of priority issues in a number of countries as regulatory authorities seek to address cybersecurity threats and enhance cyber resilience. As a central bank and a regulator in the financial sector, the SARB would be remiss in its duty if it ignored the growing risks emerging from the financial services sector's increasing reliance on cyberspace and the Internet. Because of its access to capital, the financial sector is a key target. Cyber-related attacks are therefore more likely to be directed at financial systems, institutions, and their customers. Hackers' attacks are also becoming more sophisticated as their understanding of the value chains in financial services improves.

At an international level, global standard-setting bodies – such as the International Organization of Securities Commissions as well as the Committee on Payments and Market Infrastructures – recently issued a document titled *Guidance on cyber resilience for financial market infrastructures* that should be used to address the cyber resilience of FMIs. While these guidelines are aimed directly at FMIs, it is important that FMIs actively reach out to their participants and other relevant stakeholders to promote the understanding and support of resilience objectives and their implementation.

---

1 Carney, M. *Enabling the FinTech transformation: revolution, restoration or reformation?*

2 Bradshaw, S. December 2015. *Combatting cyber-threats: CSIRTs and fostering international cooperation on cybersecurity.* Paper Series No. 23. Chatham House: the Royal Institute of International Affairs.

3 Society for Worldwide Interbank Financial Telecommunication.

The guidance document covers themes such as:

- situational awareness to understand and pre-empt cyber-events;
- collaboration to drive resilience in support of broader financial stability objectives;
- cyber-governance to implement and review the approach to managing protection against cyber-risks to ensure effective security controls that protect confidentiality; and
- the integrity and availability of assets and services as well as the testing of the elements of the cyber-resilience framework to ensure their overall effectiveness.

These guidelines will have implications for the way in which we exercise oversight over both national and regional payment FMIs, the way in which we regulate and supervise the financial institutions under the SARB mandate, as well as the way in which we monitor financial stability. At a domestic level, the bankers among you would have noted that this year cybersecurity is one of the flavour-of-the-year topics that the Bank Supervision Department of the SARB will cover in its annual engagements with the boards of directors of banks.

Motives for cyberattacks are, however, not limited to theft and often extend into a more sinister realm. Regulatory authorities must consider the possibility of systemic risks in the financial ecosystem, such as hackers bringing down a critical financial infrastructure for a prolonged period of time and the consequences of such an event. To this end, the SARB has established the Financial Sector Contingency Forum (FSCF), in which all the major financial sector stakeholders are represented. One of the responsibilities of the FSCF is to put contingency plans in place for such eventualities.

But that is not enough. We must do more, which brings me to the purpose of this conference.

The purpose of this conference

Against the background of an expanded mandate, as described in the FSR Bill, the SARB has taken the initiative to organise this cybersecurity conference. Given the potentially systemic impact of new innovations, the SARB does not take cyber-threats lightly and it is serious about deepening cyber resilience in the financial services sector. The selection of the theme for this conference – “Collaboration for building cyber resilience” – has been deliberate. We want to galvanise collective thinking and action around cyber resilience and facilitate the emergence of appropriate measures to counter common threats. We also cannot address this problem in isolation. In a highly interconnected world, our cyber-defences are literally as strong as the weakest link. All role players – from critical infrastructure operators and financial firms through to technologists and law enforcement agencies to regulators and vendors – need to work together to counter the dangers that we face.

We need to extend the focus beyond the mere reporting of cybersecurity incidents and recovery times. The whole industry needs to become more proactive in its approach and embed a healthier cyber-culture in each firm. This proposed culture will have to be risk-based and inclusive. More prominence will have to be given to greater deterrence, early detection, regular penetration testing, and quicker response times. How we strengthen our computer security incident response teams (or CSIRTs) and coordination centres becomes important. To be effective, we need to coordinate our efforts and work together.

The SARB believes that cybersecurity is a terrain with enough non-competitive and mutual interests, where public and private stakeholders can collaborate to build the resilience that is required against a common threat. A number of countries have cybersecurity frameworks in place to deal with cyber-threats. While there is a significant amount of variation and overlap across national frameworks, an important shortcoming is often the lack of coordination and cohesion at national and regional levels. We should avoid this. Indeed, there are hurdles that we will have to overcome, including privacy concerns, trust deficits, and the lack of expertise.

But these are not insurmountable obstacles. I hope you will engage fruitfully on these matters of coordination and cohesion in your deliberations and arrive at workable solutions.

Cyberattacks know no national borders. We have thus called on knowledgeable experts, both local and international, to address us on a number of relevant topics, ranging from the nature of the threat landscape and regulatory approaches to cybersecurity through future cyber-defensive tools to emerging cyber-resilience trends. To make matters a little more practical, I believe that you may examine one or two case studies and consider how to build cyber resilience into FinTech innovation. I am sure that you are also looking forward to learning how cyber-threats are addressed by the other central banks represented here and the latest developments in this regard.

Conclusion

I encourage you to explore and share your ideas on cybersecurity candidly, and I wish you well as you work on the important details of collaborating on, and laying the foundations of, effective and efficient resilience against the cyber-threats of today and of the future.

May you remain forever vigilant.

Thank you.