**Spotlight:** Financial sector innovation and cybersecurity risks

Cenfri, with support from GIZ and in collaboration with On Think Tanks, is hosting a series of digital dialogues to explore issues at the intersection of digital governance, digital financial services (DFS) and the Sustainable Development Goals (SDGs) across emerging economies. The first dialogues will cover:

- Responsible deployment of AI in financial services
- Financial sector and data innovation and cybersecurity risks
- DFS for transparent supply chains
- Digital currencies and illicit financial flows

This note puts the spotlight on the second topic, namely **Financial sector innovation and cybersecurity risks.**

Innovation in the development and roll-out of DFS in emerging markets, including Africa, has substantially unlocked financial inclusion, with 515 million new adults opening accounts in the three years leading up to the latest Global Findex survey. However, challenges persist. Poor digital literacy, limited trust in financial institutions, infrastructure constraints, capacity gaps and budgetary shortfalls all challenge the scale of innovation, as well as the ultimate impact on consumers’ lives.

To this is added the significant threat of fraud and breaches in consumer data due to cybercrime. Security has always been one of the major pillars of financial institutions and this is even more relevant in the digital age. Cybercrime is exposing DFS providers to a range of risks, such as the risk of social engineering, where people are tricked into revealing sensitive information. Criminals also use malware to hold institutions to ransom, or launch denial of service attacks – overwhelming the DFS provider with requests until the system crashes – to damage the reputation of the business, deny customers access to their accounts or to distract from an attempt to gain access to the system. The threat is real: for example, in 2020, a credit bureau attack in South Africa compromised the personal information of an estimated 24 million South African individuals and 800,000 businesses. These security breaches directly undermine consumer trust in DFS.

**How can one manage cybersecurity risks while facilitating innovation, so that more customers are included, through better services, without compromising the protection of customers or financial institutions?**
In addressing this challenge, a number of key questions are emerging:

**What is at stake if cybersecurity risks are not addressed?**

Does the provision of financial services by non-traditional providers, including fintechs, mobile network operators, services delivered via platforms and the so-called Big Tech players, pose new forms of cyber risk that require a different regulatory response or approach? What is the impact on consumer trust and how will that affect financial services access and usage? Do cyber risks differ from nation to nation and region to region, and what are the unique considerations in the developing country context?

**What should the regulatory and supervisory response be?**

How should these risks be managed – and what knowledge gaps should be bridged and what capacity built in order to adequately do so? What specialist cybersecurity skills are needed to help mitigate cyber risks and reduce financial service providers’ vulnerability? These questions are front of mind for national regulatory authorities, but also have regional implications, as cross-border trade in services mean that risks spread regionally. How should differing levels of vulnerability in a region be handled? And more broadly: how do we ensure that any approach adopted at a regional or country level is fit-for-context, rather than a mere copy and paste of developed country frameworks?

**What should be avoided in regulating and implementing cybersecurity?**

Is it likely that strict regulatory measures associated with cybersecurity risk will limit or restrict the demand or supply of financial services? What are the potential unintended consequences of improved cybersecurity measures and how could those be minimised? How can expectations around cybersecurity be aligned between financial service providers and regulators? Answering these questions again asks for an appreciation of the unique country and regional context.

**What will a collaborative solution look like?**

What are the most effective ways for financial sector stakeholders – policymakers, service providers, industry bodies, development practitioners and researchers – to share best practice in tackling cybercrime, building capacity to prevent attacks and managing the consequences? How can global-regional-local feedback loops that build globally relevant and locally appropriate solutions be ensured?

These are some of the questions that will be important to consider to strike the balance between innovation and protection that is needed at the frontier of DFS in emerging markets. The New Nexus convening on financial sector innovation and cybersecurity risks will bring together development partners, researchers, and technology, regulatory and policy experts to consider what this means in practice.

The convening is hosted in collaboration with the Africa Digital Financial Inclusion Facility (ADFI) established by the African Development Bank. ADFI works to catalyse greater digital financial inclusion across Africa, driving joint investments in digital infrastructure, digital products and innovation and policy and regulation to include 332 million Africans – 60% of whom are women – in the digital economy for the first time. ADFI is establishing the African Cybersecurity Resource Centre (ACRC) for Financial Inclusion to tackle cybercrime across Africa and to strengthen the resilience of digital financial ecosystems. For more information on ADFI and their work at the ACRC, please visit [www.adfi.org](http://www.adfi.org) or email j.akogbeto@afdb.org. To participate in exploring the topic of financial innovation and cybersecurity, please contact karenk@cenfri.org or mishkah@cenfri.org.