Risk-Based Supervision for Inclusive Digital Financial Services

TRANSCRIPT: Prudential Supervision for Data and Cyber Security Related Risks

Let's explore some of the main operational risks associated with data and cybersecurity. For each, we will identify the risk and discuss what supervisors can do to mitigate it.

Let's begin with **ICT infrastructure risks**.

A cyber incident at a financial service provider or country's critical infrastructure could generate financial stability risks through three key channels:

- loss of confidence in the provider and broader system,
- lack of substitutes for the services rendered, and
- interconnectedness of providers creating systemic issues.

Ongoing rapid digital transformation and technological innovation further increase exposure to cyber and data risks, including reliance on third parties like cloud services, open APIs, and digital customer onboarding.

Weak encryption protocols, inadequate access controls, or insufficient vendor due diligence in any of these areas can expose sensitive data to interception or misuse. Inadequate security measures can also result in unplanned downtime, or allow in malware or ransomware that blocks access to systems, which would result in reduced, inefficient, or erroneous processes.

So, what can supervisors do?
Supervisors need to ensure that financial service providers are protecting their systems from attack.

To mitigate these risks, supervisors should ensure that DFS providers implement proper **third-party risk management frameworks that also cover** critical ICT functions. Supervisors need to instill a **cyber incident reporting regime** with clear timelines and thresholds to enhance sector-wide situational awareness.

Another main operational risk is **cyber fraud**.

Falling victim to a scam or system errors can cause financial and psychological harm to customers. It can also affect a customer's confidence in financial services. Research on low-income mobile money users shows that network or service downtime is one of the greatest annoyances and leads to risky behaviours that expose users to fraud.

Vulnerable populations are particularly susceptible to fraud and access errors that can result from a cyber incident. They are often less aware and less educated about social engineering attacks. They are also more likely to use less secure channels and can least afford losses. Another added factor is that, in

emerging markets and developing economies, customers are often liable for losses associated with a cyber incident, or they bear the burden of proving that they were the victim.

So, what can supervisors do?

Supervisors should examine whether DFS providers implement **robust complaint resolution mechanisms** and **liability-sharing frameworks** for cyber fraud. Supervisors should also advocate for public disclosure of service reliability metrics, which can also promote accountability and consumer trust.

The next key risk related to data and cybersecurity is **reputational risk**.

Trust in financial service providers and payment systems is essential, and cyber incidents and their associated losses can hinder efforts to expand access to financial services. Negative experiences of customers can spread quickly and can damage DFS providers' reputations.

Such reputational damage is a risk owing to the time and effort needed to rebuild people's trust.

So, what can supervisors do?

Supervisors can develop **crisis communication protocols** that require prompt disclosure and coordinated messaging from DFS providers. This is especially after major cyber incidents to maintain systemic confidence and minimise misinformation.

Data risks are another important risk to be aware of in relation to cybersecurity.

Frequent cyberattack types include social engineering, and insider threats. The most common cybercrime-related threats are data breaches, identity theft, and fraudulent transfers. Cyber or internet fraud targeted at consumers may compromise text messages, emails, or phone calls. Such communications involve social engineering, which usually involves tricking customers into sharing personal information for account takeover or identity theft. These transactions may show up as unauthorised transactions being made from their accounts.

So, what can supervisors do?

Supervisors need to ensure that financial service providers employ cyber and data security that **protects data**, especially sensitive data and personally identifiable information, from unauthorised access.

Supervisors can establish sector-wide testing and simulation programs (such as cyber-resilience stress tests). Such testing will evaluate the financial service providers' readiness against common attack vectors like phishing, ransomware, or DDoS attacks. Supervisors can then issue minimum standards for endpoint and data protection.

Supervisors need to ensure DFS providers implement end-to-end encryption, strong multi-factor authentication, and continuous monitoring of data access to detect anomalies early.

So, we have now explored how to address these individual risks, but let's look at a broader approach in addressing data and cyber related risks.

Addressing data and cyber related risks

DFS providers, customers, and financial authorities all face challenges in adjusting their behaviours, processes, and policies to appropriately address the growing risk of cybercrime and technological failures. The constant evolution of cybercrime means all role players need to stay alert and up-to-date on developments to adequately mitigate the risks.

Supervisors' role

Supervisors need to integrate protecting data and protecting the financial systems from cyber attack into prudential regulatory and supervisory frameworks. By doing so, they link compliance to risk management and licensing conditions for DFS providers. Supervisors could also mandate independent audits of cybersecurity controls, which would be useful for supervisory assessments.

DFS providers' role

DFS providers should maintain comprehensive data security management programs. These programmes need to cover: risk assessments of data flows, data retention and deletion policies, as well as alignment with international standards. Providers also need to develop incident response plans that include data breach notifications.

Cyber security risks in emerging markets and developing economies

DFS providers and supervisors in emerging markets and developing economies face additional challenges. Despite showing growing interest in mitigating cyber security risks, they often lack access to affordable cybersecurity support and timely information on threats and best practices. There is also a shortage of qualified IT and data security professionals, especially in emerging markets and developing countries.

Supervisors working in these countries are increasingly aware of the growing cybersecurity issues and the need for urgent action. Many are developing frameworks to supervise the sector and protect their own systems. Supervisors should prioritise capacity building for staff on cyber risk supervision, including partnerships with regional training centers or international bodies such as the Bank for International Settlements (BIS), the International Monetary Fund (IMF), or the International Telecommunication Union (ITU).

Public–private collaboration can help address these gaps through joint consumer education, shared cyber threat intelligence platforms, and regional data protection frameworks that define accountability. This coordinated approach can reduce fragmentation and ensure consistent minimum standards for cyber resilience.

Supervisors can play an important role by spearheading cross-border supervisory colleges or regional cyber information-sharing forums. These colleges and forums can exchange threat intelligence and coordinate responses to transnational attacks. They may also promote certification programs for cybersecurity professionals to help reduce the local talent gap.