

Maturity of cyber security

When considering cyber security, banking institutions should remain abreast of evolving regulatory direction. Sheikh Shadab Nawaz describes how they can adapt their strategies appropriately and allocate necessary resources to satisfy compliance demands – without creating inflexible controls.

Banks in the Gulf region are probably at the forefront in terms of investing in cyber security capabilities. This is mainly driven by the following factors:

- Banks inherently tend to have minimal appetite for cyber risk
- The myriad local and global regulations that have to be complied with, depending on the jurisdictions in which they operate
- The variety of hackers potentially targeting banks and the wider financial services sector, including nation state actors, organized crime groups, hacktivist groups and individual hackers
- The imperative to build strong digital capability for customers across all channels, with the need for securing complex business inter-dependencies by connecting authorities, partners, vendors and suppliers within the banking ecosystem.

These factors represent the increasing gravity of cyber risks posed to banks, but also indicate a promising shift in the cyber-risk management approach adopted by banks operating in the United Arab Emirates (UAE).

Currently, the more progressive banks recognize cyber security is not purely a 'technology problem' but rather a wider business challenge that requires business ownership and strategic development, with clear, aligned support from technology teams. These banks tend to have their information-security risk management processes closely integrated with the overall enterprise risk management framework, to ensure every risk decision is made based on their defined-risk appetite. Chief Information Security Officers (CISOs) have generally reoriented their focus from just 'keeping the lights on' to being fully cognizant of the business side of these issues.

We also note a push for business ownership of the cyber function, by linking it more directly to business risk, and justifying the necessary levels of investment as an integral part of the banks' strategy to harness digital opportunities.

A tricky regulatory landscape

Regulatory authorities have generally identified the cyber agenda as a priority. Banks in the UAE share a common challenge in managing mounting global, regional and local regulations that can create cumbersome compliance obligations. Prominent local regulations include the UAE Central Bank's (CBUAE) requirements to comply with the information assurance standard, the strengthening of digital channels, and implementing card-security roadmaps.

While the CBUAE now frequently issues notices related to cyber security, some banks can find it difficult to connect the dots and identify priorities. It released multiple relevant circulars in 2019, on topics including:

1. Compliance assessment vis-à-vis UAE information assurance standard (CBUAE/BSD/2018/2510)
2. Credit card/debit card/ATM card/pre-paid card security (CBUAE/BSD/C/2019/2094)
3. Email and internet security (CBUAE/BSD/N/2019/2095)
4. Security of banks' digital channels e.g. internet, mobile, etc. (CBUAE/BSD/N/2019/3793).

The above circulars mandate multiple cyber security controls spread across multiple areas or domains. Some of the controls are repetitive e.g. vulnerability assessment and penetration testing control in CBUAE/BSD/C/2019/2094 is reiterated in CBUAE/BSD/N/2019/3793. Banks are finding it difficult to keep track of the large volume of circulars and prioritize implementation of relevant policies. However, we understand that the CBUAE is mainly focusing on the

first circular at this point in time and has asked all banks to submit a report by the end of March 2020.

In our experience, it appears most banks and other financial institutions in the UAE have assessed the extent of their compliance with the UAE information assurance standard and obtained management commitment to implement the steps required to achieve compliance.

While “security by design” is the mantra for most leading banks operating in the UAE, some banks are still fettered by the boundaries of “security by compliance.” This latter approach can no longer be sufficient, as exposure to potential financial fraud like corporate payment processing breaches, retail customer account hacks, and fraudulent transactions to unknown accounts are no longer the only cyber risks banks must consider. The emergence of innovations like open banking, the second Payment Services Directive (PSD2), blockchain-based customer transactions, and artificial intelligence (AI) based smart platforms have the potential to transform the banking ecosystem and require an agile, continuous integration and delivery approach to customer security. Banks therefore ought to rethink their internal controls to secure digital banking solutions and detect and deter fraud.

The limitations of security by compliance

Within the UAE banks, there can be marked convergence between cyber, anti-money laundering (AML) and fraud-risk management, as financial institutions begin to tackle these issues in a more integrated and holistic manner. There is also greater management focus on cyber security operations, and revamping Security Operations Centers (SOCs) to create more dynamic defenses and to better leverage cyber threat intelligence.



Some banks have achieved encouraging results through training employees to develop cyber scenarios, thereby building an understanding of the nature of cyber incidents and their impact on the business. These banks are tailoring information-security training to raise awareness of specific threats (including gamification that engages their audiences), rather than providing standard training.

We have seen an increase in cyber simulations with an organization-wide focus. These are aimed at increasing cyber-security awareness among senior management, business users and technical teams. They also serve to assess the effectiveness of existing incident detection, and response and recovery plans. Typically, these simulations are delivered through an advanced online-simulation platform.

We have also observed a greater focus by banks on the cyber risks arising from third-party service providers (partners, vendors and

suppliers). They have been evaluating the security controls of these vendors, scrutinizing what data are being shared with outsiders, and conducting cyber-security simulations that involve testing the suppliers’ connections and personnel.

There is also a great degree of collaboration and intelligence-sharing amongst banks in the UAE, and increasingly amongst regulators. This trend is likely to mature and include the wider community: an immensely positive development that reflects our view that cyber risk is not solely a technology problem but one that must be addressed from a business perspective.

Sheikh Shadab Nawaz
*Director
Digital & Innovation
KPMG Lower Gulf*

