Increased expectations of data privacy

Cybersecurity and data privacy are often seen as different disciplines that operate in silos. However, in an environment where so much sensitive data is captured and utilized, the review of third parties, new systems, and new applications requires a multidisciplinary approach that includes both privacy and security from the design phase through to organizational change management.

Regulatory environment

In 2017, SAMA established a Cyber Security Framework to enable Financial Institutions to identify and address cybersecurity risks. The Framework is based on the SAMA requirements and industry cybersecurity standards, such as NIST, ISF, ISO, BASEL and PCI.[34]

In addition to cybersecurity, global awareness for individual right and privacy has increased leading to global regulations such as the General Data Protection Regulation (GDPR) in Europe to various individual regimes across Asia, North and South America. Saudi Arabia is the latest nation to act, with its Personal Data Protection Law (PDPL), which was set to go into effect on 23 March 2022, but which enforcement is postponed till 17 March 2023. PDPL applies to all corporations and public and private entities operating in the Kingdom. This new timeline should be considered as a opportunity for all entities to start preparing now.

The PDPL will be supervised by the Saudi Data and Artificial Intelligence Authority, which also developed it, and applies to the processing of personal data within Saudi Arabia and also to the handling of residents' personal data outside the Kingdom. Data transfers out of the Kingdom will also be tightly controlled.

Risks to banks

The banking industry is based on trust, so the main risk of cybersecurity threats is compromising the trust of clients. This risk manifests itself within every transaction in the form of money being stolen from banking accounts or other kinds of fraud, which are now within the digital context since money is not physically in the branches but in the IT systems.[35]

Data privacy concerns also come into the foray of risks faced by banks since they hold a lot of sensitive information on clients and they have the responsibility to protect it. With this, there is a threat of someone trying to obtain and use this information illegally.

Saudi Arabia has faced increasing security threats, especially with Covid-19 and remote working.[36] The financial services industry faces most of these cyber attacks, which increasingly target multiple banks simultaneously. Evidence also suggests that attacks on financial institutions are becoming more complex, since they have valuable and voluminous data, which gives cybercriminals the opportunity to monetize their work.[37]

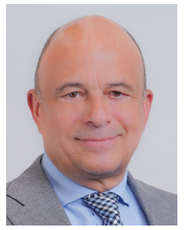
The key threats to cybersecurity and data privacy the Kingdom include:

- **Advanced phishing:** machine learning is used to quickly craft and distribute convincing digital messages which increase the threat of malware and exposure of sensitive data.
- **Internet of Things (IoT) interconnectivity:** proliferation of insecure devices on an IoT network, coupled with legacy systems, are making businesses highly susceptible to cyber-attacks and data breaches, as accessing one device opens the flood gates to accessing all devices on the same network.
- **Data infrastructure:** both cloud and physical data storage have cyber security challenges. Physical data storage facilities are susceptible to targeted attacks while cloud infrastructure can be targeted by cyberattacks.[38]

Key actions for banks to consider

- To mitigate threats and to comply with the new PDPL, banks must make significant changes to the way they collect, store and process personal data, they must prohibit certain practices, and establish a complaints procedure.
- They can adopt a privacy-by-design standard to supplement and complement the rules, regulations, and regulatory expectations around privacy.39
- They should strive to educate senior and business management on respecting consumer rights and obtaining consent for data collection.
- They can utilize AI technology to automate processes that recognize, monitor, and analyze transactions to protect capital and sensitive information. This can help banks comply with regulations, increase response speed, and reduce human error.
- AI and machine learning can also be used to secure cloud environments against malware penetration.

Data privacy concerns also come into the foray of risks faced by banks since they hold a lot of sensitive information on clients and they have the responsibility to protect it.



Ton Diemont
Head of Cybersecurity & Data Privacy
E: antondiemont@kpmg.com