Evolving environment

Key cyber considerations

In line with the acceleration of digitalization and remote work, the prevalence of cybercrime has increased during the Covid-19 pandemic. For banks, the threat is pronounced and growing. Luckily, the sector has been at the forefront of cybersecurity for years and has thus been well-guarded from new threats posed by cyber perpetrators. The cybersecurity landscape is rapidly evolving, and there are several key developments that are shaping cyber in the banking sector.

Open banking

Open banking is a practice that provides third-party financial service providers open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions using application programming interfaces (APIs). It also allows for greater financial transparency for customers and uses open source technology to build the ecosystem. At each level, cybersecurity measures and policies will determine the success of open banking.

In a January 2021 policy paper, the Saudi Central Bank (SAMA) announced that it is developing an "open banking initiative" intended to help shape the rules around open banking and promote its healthy use as the fintech sector develops. SAMA plans to "go live" with open banking during the first half of 2022, after its design and implementation phases are complete.

As stakeholders in the Kingdom develop their own open banking initiatives, they should recognize the importance of security. All third-party providers have to comply with regulator and bank data protection rules, which should be focused on customer privacy protection. The provider must inform the bank and the customer what data it intends to use and how it will use it, as well as how long it will remain within their system.

> Banks will have to better understand their data practices and the impact of new regulations on their business strategies and business models.

Internal risks

Cyber in the Audit (CitA) provides a framework and guidance for a structured approach and risk-based decision making for assurance. Traditionally, auditors have tested their clients' general IT controls (GITCs). However, as risks evolve, so too does the role of the auditor. Just as an IT audit supports a financial audit by testing automated controls, CitA supports the IT audit by testing the cybersecurity measures in place to prevent an attack on an IT system. The emphasis for CitA is a forward-looking approach where the controls are designed to provide an assurance on the IT dependencies that a bank relies upon. It gives insight into a bank's cybersecurity controls and makes plans for, in case of a cyberattack or compromise, what steps need to be taken to respond and recover.

Data Privacy

Whether a bank started its privacy journey because of a regulation or as an initiative, privacy is now firmly a sector-wide priority. Full engagement across the bank is key as privacy professionals look to embed privacy into the DNA of business operations and customer engagement.

Banks must chart a plan that not only encompasses the immediate regulatory challenges, but also a plan for a shifting regulatory climate and consumer expectations of greater individual control of

data. In creating a sustainable and effective data protection strategy, companies should develop a solid framework of best practices and infuse those practices—both procedurally and culturally.

While data should be viewed as a valuable asset, it should not be seen as such in and of itself. It is what a bank does with its data that gives it value – like creating better customer experiences and offering customized products. Additionally, businesses that proactively manage and protect personal data the way users expect will come out ahead of their competition. Banks will have to better understand their data practices and the impact of new regulations on their business strategies and business models. Waiting to the last minute is not a viable option, because the goal is building customer trust and loyalty.

Penetration Testing & Red Teaming

Though better prepared than most sectors, the banking sector still lags behind the cyber threats landscape. Hackers will find opportunities to exploit flaws in the way banks currently fund, manage, enable, organize and implement their information protection capabilities. Thus, it is important to stay ahead of the threat by testing what your defenses are capable of.

Accordingly, banks are expected to take action, best by simulating potential cyber attacked, for example from real attackers (including phishing and malware), testing the Tactics, Techniques and Procedures (TTPs) and the overall incident response and threat management.

Secure DevOps

DevOps is a philosophy based on combining the traditional roles and responsibilities of development teams and IT operations teams to accelerate the delivery of business value through the two teams. When work flows smoothly through development and IT operations, new software features come to market more frequently and the business becomes more competitive and adaptive in a constantly shifting market.

The central concept of Secure DevOps is the integration of security into the development and IT operations teams. By adding security into the original mix, the velocity for security changes increases as well. The likelihood of vulnerabilities being introduced is reduced, and banks are able to more quickly mitigate risks that remain. It is paramount that banks focus on custom implementations for their environment and goals. This includes discussing tangible actions within IT, development and security to enhance the existing culture, processes and technologies in the transition to Secure DevOps capabilities. Across the three groups, necessary changes to the cultures of the groups are similar. Because of the vast changes to various processes, the individuals involved must be willing to undertake new programs and processes and different approaches to traditional work. And because of the assortment of new processes and technologies adopted in order to support Secure DevOps, it is crucial banks encourage their workforce to share challenges and failures.

Ton Diemont
Cybersecurity Lead
KPMG in Saudi Arabia

Ton Diemont has vast experience in cybersecurity, IT and Operational Risk Management and Financial Services. He worked over 21 years with leading financial institutions in the Netherlands, most recently as CISO. He worked with many central banks, regulators on the implementation of cybersecurity measures and risk governance customer-centric transformation programs.