Cyber security: beating the challenge

With the rapid growth of Financial Services technology and the adoption of electronic channels, money is increasingly moving in a digital manner. But along with the advances we have seen a marked increase in cyber-security breaches and fraud. What can banks do to meet the challenge, asks Sheikh Shadab Nawaz.

The pace of technology-enabled innovation has increased exponentially over the last decade, resulting in new business opportunities in the banking industry, such as digital branding (via mobile and internet channels), Augmented Reality (AR) and Virtual Reality (VR)-based banking channels, blockchain-based transactions and the Internet of Things (IoT)-based payments. Transactions are being processed faster, free, and in a user-friendly manner.

These evolutions have fundamentally changed the way customers expect to interact with banks. They now demand an omni-channel presence, improved client experience, secure transactions, and better control over fraud and data privacy.

These issues have made cybersecurity one of the top ten priorities in the board room, as any breach could undermine the trust that customers have in their bank, and therefore affect the future profitability and sustainability of the organization. Banks in the UAE are no different and are ready to make suitable investments in cybersecurity. They should consider investing in cyber security from a consumer-centric point of view. Based on our global expertise of delivering cyber-security solutions and our experience of creating digital solutions for banks, we believe there are seven key capabilities that are strategic to secure digital solutions for clients and build greater trust in the organization:

- **Cyber specifics**: Cyber security strategy & governance and cyber security defense & response are the traditional blocks of security. These translate into a number of specific areas, as follows:
  - **Consumer Identity and Access Management**: Provides a single identity across multiple channels for users to access their accounts, manage their preferences, and manage their credentials in a secure manner. It also provides a mechanism to gather data to understand customer needs and preferences.
  - **Advanced Authentication**: Changing technologies and increased security concerns have almost rendered passwords obsolete. In order to meet both security and customer requirements, multiple, advanced authentication options, such as biometrics and push notifications, will likely need to be offered. Higher assurance credentials can be leveraged to increase the security assurance of a user for higher risk transactions, such as balance transfers and trades.
New technologies, such as cloud and mobile, are driving customers to want to access their accounts from any channel, at any time, from anywhere. This is resulting in significant changes in architecture. In order to adapt to these changes, security ought to be designed into the architecture and development lifecycle, across different channels and technologies.

The proliferation of different devices poses new security risks. Understanding and adapting to the security of different devices and digital interfaces that the consumer connects with is essential to minimizing account takeover and malware introduction.

As digital financial transactions are becoming more commonplace, securing the mechanisms that enable each transaction is critical to successfully compete in the omni channel and completely mobile environment.

**Up close and personal**
Banks handle a significant amount of personal information. Although regulations for handling this data varies from region to region, any personal information collected should be managed in accordance with the local regulations and only used with the consent of the owner of the information.

Understanding how regulations, such as the UAE National Electronic Security Authority (NESA), EU General Data Protection Regulation (GDPR) and others, play a part in the organization’s digital strategy is essential in order to succeed and outpace competitors. Increasing regulatory pressure from the US, the UK, Europe and elsewhere require adjustments in technology configurations, and security requirements are increasingly being enforced. New global regulatory pressures will play a significant role in how Financial Services institutions interact and collect data on their consumers. This needs to be aligned and understood with the overall organizational digital strategy.

In our 2017 UAE CEO Outlook survey (https://assets.kpmg.com/content/dam/kpmg/ae/pdf/UAE-CEO-outlook.pdf), it was clear that chief executives would be paying more attention to – and investing more in – cyber security in coming years. Yet finding staff with appropriate skills is a challenge: as many as 84% of UAE CEOs reported that human capital is currently one of the biggest challenges they face when it comes to tackling this issue. These CEOs, however, believe that such risks, if tackled adequately, can further prompt innovation in products and services.

UAE CEOs are more likely (84% compared with 53% of their global counterparts) to see cyber security as a way of prompting product and service innovation. Over two-thirds see investment in cyber security as an opportunity to generate new revenue streams and innovate, rather than being just an overhead.

We don’t think there are many board meetings or executive meetings in the UAE where the cyber threat isn’t discussed. If companies aren’t concerned, they probably should be.

**Sheikh Shadab Nawaz**
Associate Director | Head of Cyber Security, IT Advisory
T: +971 4 424 8973
E: snawaz1@kpmg.com

Shadab has thirteen years’ experience in cyber security; information technology (IT) governance, risk and compliance (GRC); data, software and cloud security; and IT Disaster Recovery. He has worked on over 100 complex technology projects across a number of industry verticals, including banking and financial institutions; telecommunications; retail; oil & gas; aviation and government. He has been based in the Middle East, India and South East Asia.

Shadab holds a bachelor’s degree in electrical engineering, a master’s in IT and a post-graduate diploma in systems management. His current research interests focus on security analytics, breach investigation and cyber insurance.

“If companies aren’t concerned, they probably should be”