ERIC KRAWETZ
ASSOCIATE CONSULTANT
HKA

MAJDI AL-MADANI
PARTNER
HKA

The Growth and Development of Saudi Arabia's Cybersecurity Landscape

Financial services firms around the world continue to wrestle with cybersecurity risks such as data breaches, business interruption due to ransomware and other attacks, and monetary losses from wire fraud. Private industry, governments, and regulatory bodies struggle to keep pace with the cyber threat landscape. According to Cybersecurity Ventures, damages from cybercrime are projected to reach $6 trillion in 2021, and rise all the way to an astounding $10.5 trillion (annually) by 2025. Financial services institutions continue to be in the crosshairs of an evolving cyberattack landscape.

Vision 2030 and the Digital Transformation in Saudi Arabia
While the United States has consistently been a global leader in cybersecurity, the Kingdom of Saudi Arabia (KSA) has only recently emerged as a front runner in this arena. The Global Cybersecurity Index 2020 (GCI), a measure of the commitment individual countries have to cybersecurity, ranked the United States first and KSA second. The global rank of KSA advanced tremendously from 46 in 2017 to 13 in 2018, as a result of the country's heightened commitment—through new regulation and programs—that require financial services firms to improve their cybersecurity posture and maintain minimum standards.

Implementing Vision 2030 and the National Transformation Program 2020 put KSA at the forefront of positive change in the area of digital transformation. In 2016, Saudi Arabia's Vision 2030 was adopted as a strategic framework for economic development in the public, private, and not-for-profit sectors. The National Transformation Program 2020 was initiated to help achieve Vision 2030 through the identification of potential challenges, aiding the government in establishing plans and procedures that focus on these challenges. The KSA's investment in digital infrastructure is vital to realizing Vision 2030.

This digital transformation presents many advantages from an economic and strategic standpoint, yet increased digitization has elevated the need for increased cybersecurity standards as KSA's cyberattack landscape continues to grow. As a result of these transformative initiatives, in 2017, KSA established the National Digital Transformation Unit (NDU), along with the National Digital Transformation Committee, by a royal decree. Since its inception, the NDU "aims at realizing many accomplishments through a national digital perspective that reflects [KSA's] digital vision." The NDU provides subject matter expertise to the government and private organizations to realize the strongest digital development possible through improving digital innovation.

National Cybersecurity Authority
The year 2017 marked a significant milestone for KSA, when a royal decree centralized the nation's cybersecurity risk management with the National Cybersecurity Authority (NCA) in a robust effort to align with Vision 2030. As stated on its website, the NCA was established "to protect the Kingdom's vital interests, its national security, its critical infrastructure, priority sectors, government services and activities." The NCA covers regulatory and operational functions and provides support and increased coverage to further the protection of

the Kingdom’s networks, hardware and software, information technology systems, and operating systems.

Considering these new objectives, financial services firms are expected to maintain the highest levels of cybersecurity to thwart potential threats. These firms must have robust cybersecurity programs to ensure their customer information, operation systems, and assets are constantly protected. It is paramount that financial services firms maintain the confidentiality, integrity, and availability of information to protect their business, as well as the investors.

> “Considering these new objectives, financial services firms are expected to maintain the highest levels of cybersecurity to thwart potential threats.”

NCA and the Essential Cybersecurity Controls

Cybersecurity is defined in the official charter of the NCA as “the protection of information technology systems and networks as well as systems and components of operating technologies, including hardware and software, together with services provided thereby and data included therein, against unlawful hacking, obstruction, modification, access, use, or exploitation.” In 2018, to guide organizations in implementing good cybersecurity practices, the NCA developed the Essential Cybersecurity Controls (ECC). The ECC comprises 114 main controls divided into five domains:

- Cybersecurity Governance
- Cybersecurity Defense
- Cybersecurity Resilience
- Third-Party and Cloud Computing Cybersecurity
- Industrial Control Systems Cybersecurity

To further the commitment to achieve KSA’s vision for 2030, the NCA recommends and encourages organizations in all industries to implement these controls to enhance their internal cybersecurity postures. As KSA strategically transforms its increasing digital landscape, it becomes a larger target for cyberattacks. Implementing these controls will mitigate risk and protect organizations such as financial institutions from facing losses and damages to their balance sheet and their reputation.

The Saudi Arabian Monetary Authority’s Cyber Security Framework

In May 2017, the Saudi Arabian Monetary Authority (SAMA) issued its Cyber Security Framework to empower financial institutions regulated under SAMA to address identified cyber risks and manage their findings. The framework is based on widely accepted industry standards such as those of the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the Basel Committee on Banking Supervision. The Cyber Security Framework covers four domains that financial institutions must follow:

- Cyber Security Leadership and Governance
- Cyber Security Risk Management and Compliance
- Cyber Security Operations and Technology
- Third Party Cyber Security

To measure the compliance of financial institutions in KSA to SAMA's Cyber Security Framework, SAMA's cybersecurity maturity model has defined maturity levels, zero through five. A maturity level of zero means an organization's cybersecurity posture is non-existent, and five means an organization's structured and formalized cybersecurity policies and procedures are subject to continual improvements. According to SAMA, to effectively manage internal cybersecurity programs and mitigate risk, financial institutions must operate at a level three maturity rating or higher. Achieving maturity level three is determined by formalized policies, standards, and procedures, that are implemented and routinely tested. This documentation should be monitored and key performance indicators should be defined. Upholding organizations to SAMA's Cyber Security Framework will influence growth in KSA's financial services industry, better aligning it to Vision 2030.

> "To further the commitment to achieve KSA's vision for 2030, the NCA recommends and encourages organizations in all industries to implement these controls to enhance their internal cybersecurity postures."

Reducing Cybersecurity Risk for Financial Services Companies
With respect to developing talent to help reduce cyber risk in the workforce, the Saudi Federation for Cybersecurity, Programming and Drones was established to contribute to such development through its initiative of providing cybersecurity education for students. It is well documented that the global market for cybersecurity professionals is quite strained, given that the demand for qualified and experienced professionals greatly exceeds the supply. Many companies do not have the proper in-house expertise to perform the cyber-related tasks necessary to maintain an adequate cybersecurity posture. Some businesses, such as financial institutions, have thus resorted to outsourcing cybersecurity services to third-party cybersecurity teams. Regardless of the approach, it is vital for the business operations of financial institutions to proactively and routinely manage their internal cybersecurity framework.

HKA's Cybersecurity Risk and Privacy team has decades of combined experience in the cybersecurity industry. Providing personalized expert advisory services, HKA will assess an organization's current cybersecurity and privacy posture for areas of improvement. HKA's expert advisory services include risk management, governance, and compliance; third-party and vendor risk management; incident response; retrieval and analysis of data; and awareness and training. Serving a multitude of industries, HKA uses a small team of experienced, focused investigators to achieve an efficient and cost-effective result. HKA's cybersecurity experts have a profound understanding of internal operations and can help mitigate the risk of future cyber threats.

If you require any further information, please contact Eric Krawetz at erickrawetz@hka.com or Majdi Al-Madani at majdialmadani@hka.com.

HKA