مجلس الأعمال السعودي الأمريكي
U.S.-Saudi Arabian Business Council

January 2020
www.us-sabc.org

USSABC Economic Brief:
Saudi Arabia's Emergence in Cyber Technology

Overview

Cybersecurity is a growing global industry at the intersection of every sector and its integration with the digital economy. Saudi Arabia's cybersecurity market is expected to grow at a compounded annual growth rate (CAGR) of 16.59 percent between 2018 and 2023, representing the largest market in the Middle East. Saudi Arabia has undergone rapid ICT adoption in the past fifteen years and has been a growing target for cyber threats. These threats are expected to increase as the Kingdom undergoes a digital transformation and evolves towards a knowledge economy.

Saudi Arabia has responded by modernizing its information security governance, growing cybersecurity spending, and providing support for private sector entry into the cybersecurity field. The Kingdom was recently ranked by the International Telecommunication Union (ITU) as the top regional cybersecurity industry and the top reformer in capacity-building. The proliferation of network-connected devices, cloud storage, and new technologies present additional challenges and new business opportunities in the cybersecurity industry.

The Cybersecurity Landscape

Technological integration and mass data storage via cloud sharing are becoming commonplace in business, necessitating new security protocols to address growing vulnerabilities. Market estimates predict that between 50 to 60 percent of firms will experience a cyber attack in the next twelve months. The public sector, healthcare, and finance are the most frequently targeted sectors while education, industrial, retail, and energy are also heavily targeted. The majority of attacks involve phishing while malware, ransomware, direct denial of service (DDoS), web application attacks, and privilege abuse are also common.

Saudi Arabia's more recent and rapid technological development poses unique risks but also presents an opportunity to establish a robust cybersecurity environment based on world-class benchmarks. According to an IBM report, Saudi Arabia and the UAE had the second highest average data breach cost at SAR22.4 million ($5.97 million) in 2019. Saudi Arabia and the UAE also had the highest average number

Albara'a Alwazir
Economist
alalwazir@us-sabc.org

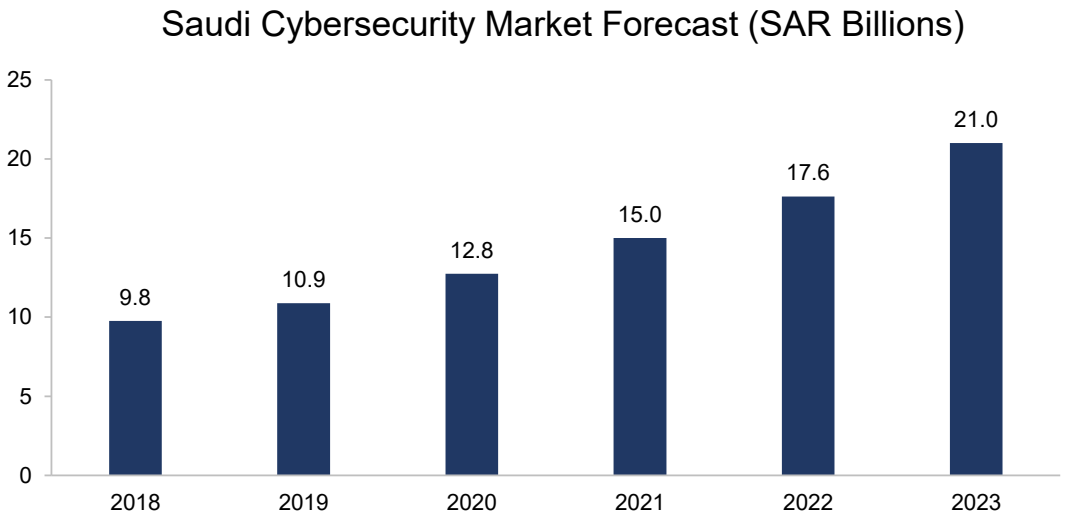
Jacob Dichter
Economic Research Assistant
jdichter@us-sabc.org

of breached records at 38,800 per incident compared to a global average of 25,500 records per incident. Saudi Arabia and the UAE took an average of 279 days to identify a data breach and 102 days to contain it compared to a global average of 206 days to identify and 73 days to contain. Between 2016 and 2018, Saudi Arabia was the sixth most affected country in the world by targeted cyber attacks.

Investment & Governance

High-profile cyber attacks such as the Shamoon attack on Saudi Aramco and Saudi Arabia's recent ICT transformation spurred a policy shift in the prioritization of cybersecurity. Vision 2030 identifies a sophisticated digital infrastructure as integral to its advanced industrial activities and the fundamental competitiveness of the Saudi economy. The National Transformation Plan 2020 emphasizes the opening of the private sector to further develop the digital economy and IT security.

Saudi Arabia's 2020 budget allocates SAR102 billion ($27.2 billion) for security and regional administration which includes cybersecurity. The size of Saudi Arabia's cybersecurity market in 2019 was SAR10.9 billion ($2.9 billion) and that market is expected to grow at a CAGR of 16.59 percent through 2023 to an estimated SAR21 billion ($5.6 billion).



Source: 6W Research, USSABC estimates

The government has not only increased its digital infrastructure investments, it has also established development and training programs for Saudi nationals and modernized information security governance. Saudi Arabia established the National Cybersecurity Authority (NCA) in 2017 to centralize cybersecurity controls and the National Cyber Security Center (NCSC) to serve as the technical and operational arm of the NCA. The NCSC monitors supervisory control and data acquisition (SCADA) systems across government entities, particularly in the energy and industrial sector.

The Communications and Information Technology Commission (CITC) is another key entity that serves as the regulatory authority for the ICT sector. CITC provides Computer Emergency Response Team (CERT) services to assist in information security incidents and issues statutory protocols such as the Anti-Cyber Crime Law which was passed in 2007. In 2019, CICT established new regulatory frameworks for cloud computing and IoT (Internet of Things) as well as guidelines for new developments such as 5G and smart buildings.

Capacity-Building & Skills Development

Saudi Arabia is actively addressing the IT and cybersecurity skills shortage through a variety of programs. In 2019, the Kingdom trained 751 employees across 113 companies as well as 288 students in specialized cybersecurity protocols. The government also offered scholarships to 231 students in cybersecurity specializations. These programs are critical to meet localization and Saudization requirements for domestic firms. In 2017, King Abdullah Center for Science and Technology (KACST) established the Saudi Research and Innovation Network (Maeen). Maeen advises Saudi organizations on regulatory compliance, offers information security recommendations, and investigates cyber attacks.

KACST's National Center for Cybersecurity Technology (C4C) as well as the Prince Mohammed bin Salman College for Cybersecurity, Artificial Intelligence, and Advanced Technologies are educational institutions established to develop national human capital in IT and cybersecurity capabilities. In 2018, the Saudi Arabian Federation for Cybersecurity, Programming, and Drones (SAFCSP) was established to spur technology innovation and provide professional development to Saudi nationals. Its programs have included cybersecurity boot camps and hackathons to encourage youth participation.

Taqnia Cyber, a subsidiary of the Saudi Technology Development and Investment Company (TAQNIA), specializes in ICT and industrial cybersecurity for private firms. The company is involved with training and capability development and aims to localize relevant technologies and meet growing demand through cooperation with national and international partners.

The Badir program promotes technical entrepreneurship by offering financing and incubation for startups in fields such as cybersecurity to meet the Kingdom's national objectives. The Soft Landing program is an offshoot program for international startups and emerging companies in technology fields to facilitate access to the Saudi market.

These recent investments and initiatives have improved Saudi Arabia's competitiveness in the cybersecurity sector. In ITU's benchmark Global Cybersecurity Index, Saudi Arabia improved from #46 globally in 2017 to #13 in 2019, emerging as the regional leader. The Kingdom's score rose from 0.569 to 0.881 where a score exceeding 0.67 indicates a high level of cybersecurity capacity and high level of national commitment to international standards, organizational and technical measures, and professional development.

Table 1: Global Cybersecurity Index 2019 MENA Regional Results

State	Score	Global Rank (2019)	Global Rank (2017)	Rank Change
Saudi Arabia	**0.881**	**13**	**46**	**33**
Oman	0.868	16	4	-12
Qatar	0.86	17	25	8
Egypt	0.842	23	14	-9
United Arab Emirates	0.807	33	47	14
Kuwait	0.6	67	139	72
Bahrain	0.585	68	65	-3

Source: ITU

Private Sector Spending

The private sector's large enterprises have substantially increased their investments in IT security as a survey by Gartner indicates total cumulative spending is expected to reach SAR7.4 billion ($2 billion) between 2018 and 2023. Moreover, enterprise spending is expected to grow from approximately SAR911 million ($242 million) in 2018 to SAR1.6 billion ($415 million) by 2023, a CAGR of 11.3 percent. The largest share of enterprise spending is on security services, network security equipment, and infrastructure investment. Alternatively, consumer spending, which reached approximately SAR86 million ($23 million) in 2018, is expected to reach SAR124 million ($33 million) by 2023. Cloud security spending is expected to dramatically grow by a CAGR of 55.2 percent by 2023 as the technology becomes more prominent in the region.

Table 2: Enterprise Cybersecurity Spending Forecast (SAR Millions)

Market	2018	2019	2020	2021	2022	2023	Total	CAGR
Application Security	23	26	26	30	34	38	176	10.8%
Cloud Security	4	4	8	15	23	34	86	55.2%
Consumer Security Software	86	94	101	109	116	124	630	7.5%
Data Security	26	30	41	53	64	75	289	23.4%
Identity Access Management	94	105	124	143	161	176	803	13.5%
Infrastructure Protection	98	113	131	150	173	195	859	14.9%
Integrated Risk Management	15	19	23	30	34	38	158	20.1%
Network Security Equipment	165	195	214	236	248	259	1,316	9.4%
Other Information Security Software	15	15	15	15	15	15	90	0.0%
Security Services	386	428	469	510	559	604	2,955	9.3%
Total	**911**	**1,028**	**1,151**	**1,290**	**1,425**	**1,556**	**7,361**	**11.3%**

Source: Gartner, USSABC

The private sector's approach to cybersecurity demands a shift away from viewing cybersecurity as a technological issue but rather an organizational pillar that is best promoted by a company's board members. With the proliferation of digital channels by which goods and services are traded along with perpetual sharing of sensitive data, the need to look beyond basic measures of cybersecurity risk mitigation is paramount. Cyber security is an IT responsibility whereby foundational frameworks should be created to account for the Kingdom's rapid expansion plans as well as constantly evolving regulatory reforms.

Challenges & Opportunities

Although successful cyber attacks on large companies attract substantial attention, 43 percent of data breaches are against small and medium enterprises (SMEs) according to Verizon. Highly targeted industries such as healthcare and finance often possess the most advanced digital security systems, but this typically characterizes only larger firms. SMEs tend to underestimate potential risk, have less robust security capabilities, and are more likely to incur irrecoverable losses from a cyber attack compared to large firms. These businesses all possess valuable intellectual property, customer records, or financial information.

In order to identify the potential market size for cybersecurity solutions, we looked at the Kingdom's SME businesses in highly targeted sectors like retail, finance, education, and healthcare. According to the General Authority for Statistics (GAStat), SMEs account for 480,326 of the 490,269 total establishments across retail, finance, education, and healthcare with retail comprising most of these firms. Other SMEs in highly targeted sectors include 2,411 healthcare establishments (58 percent of total), 6,103 finance, real estate, and insurance establishments (87 percent of total), and 6,074 education establishments (65.1 percent of total) in Saudi Arabia. Assuming the market estimate that 43 percent of data breaches target SMEs, this brings the total market opportunity to 480,326 establishments that are at risk of being targeted.

Table 3: Establishments in Sectors Highly Targeted by Cyber Attacks

Sector	SMEs	Large Firms	Total
Retail	432,106	3,811	435,917
Finance, Real Estate, and Insurance	39,735	1,130	40,865
Education	6,074	3,253	9,327
Healthcare	2,411	1,749	4,160
Total	**480,326**	**9,943**	**490,269**

Source: GAStat

According to Ponemon Institute, small businesses cite insufficient personnel (74 percent) and insufficient budget (55 percent) as the top challenges keeping their IT security posture from being fully effective. However, 47 percent of SMEs cited "no understanding of how to protect against cyberattacks." The lack of in-house expertise represents an opportunity for these businesses to collaborate with managed security service providers (MSSPs).

Additionally, these sectors have unique security needs. For example, data breaches by internal actors represent the majority of cyber incidents in the healthcare sector (59 percent) while the finance and insurance sector is more likely to face a data breach from an external actor (73 percent). The education sector has been shown to be substantially more vulnerable to spear-phishing scams while the risk is much lower in the healthcare sector where credential misuse is more common.

In addition to susceptible market segments, the introduction of new technologies create new security needs as the number of vulnerable endpoints increases. In 2020, Saudi Arabia will continue the rollout of the region's largest 5G network. While 5G technology represents a significant milestone in the Kingdom's digital transformation, 72.5 percent of businesses believe 5G will have a significant effect on their cybersecurity network and will require a new security stack according to a 2019 report by AT&T. Nearly all businesses expect to make 5G-related security changes in the next five years.

These changes, along with the proliferation of IoT technology across many sectors, will further increase the potential attack surface for businesses and institutions. A 2018 survey of private firms in Saudi Arabia showed IT security budgets growing at a rate of only 2.8 percent compared to the global average of 4.9 percent. We expect this rate to increase as the need for a robust security posture will be necessary to secure the growth of the Kingdom's digital economy across the public and private sector.