

CYBER SECURITY AND ITS IMPACT ON DIGITAL SAUDI

Prepared by:



Sponsored by:



TABLE OF CONTENT

Cybersecurity and its impact on digital Saudi



6

- 1 Saudi Arabia's Cybersecurity Landscape

16

- 2 Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape

20

- 3 Evolving Competitiveness of the Local Cybersecurity Ecosystem

26

- 4 Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

32

- 5 Initiatives & Developments to Improve the Saudi Cybersecurity Environment

38

- 6 Interview with Mobily: Securing the Kingdom's Digital Transformation Journey

44

- 7 Cybersecurity Challenges in Today's Digital World

58

- 8 Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World

64

- 9 Cybersecurity and Trust in the Era of Digital Transformation

80

- 10 Interview with Al Moëmmar Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



Foreword



Over the past few years, the Kingdom of Saudi Arabia has made significant strides in establishing itself as a global digital powerhouse. The Kingdom's commitment to embracing digital transformation is evident from the principles laid out in Vision 2030 — an ambitious reform agenda launched in 2016 that aims to transform Saudi Arabia into a digitally enabled trade, innovation, and investment hub. To bring this vision to life, the Saudi government recognizes the need for a sophisticated digital infrastructure, which is vital for advanced industrial activities, attracting investments, and diversifying the economy through the development of public service sectors such as health, education, infrastructure, recreation and tourism.

With an increased focus on digital enablement, Saudi Arabia is acutely aware of the cybersecurity threat it will face as the economy accelerates its digital ambitions. As such, the Kingdom has invested in strengthening its cybersecurity posture by implementing cybercrime legislation, robust national cybersecurity strategies, proactive computer emergency response teams (CERTs), and awareness and capacity campaigns, all of which have been complemented by local skills incubation in the field of cybersecurity.

The fact that earlier this year Riyadh hosted the first-of-its-kind Global Cybersecurity Forum – a two-day forum that brought together a range of global, regional, and local decision makers and security experts from governments, businesses, academia, and the investor community to address cyber opportunities and challenges – is testament to Saudi Arabia’s committed focus on cybersecurity.

As Saudi organizations accelerate their digital journeys, many face significant cybersecurity challenges. If cybersecurity teams are to avoid becoming barriers to digitization, they must transform. The onrush of digital technologies is inevitable as Saudi Arabia kickstarts its new wave of mega-projects (NEOM, Qiddiya, Red Sea Project, etc.) and intensifies its modernization drive to build a sustainable, investor-friendly business environment. The impetus to secure the foundations of Digital Saudi is stronger than ever and will demand high levels of collaboration, best-practice sharing, and commitment to cybersecurity.

IDC is honored to present our latest report, which showcases the impact of cybersecurity vis-à-vis Saudi Arabia’s National Transformation Program, and to reaffirm our commitment to the Kingdom and the friendships and partnerships we have established there. Our special thanks go to His Highness Crown Prince Mohammed bin Salman, the leadership team within the Council of Economic and Development Affairs, and the many ministers, leaders, and innovative thinkers that have shaped the Program and will be instrumental in delivering its full potential.

We look forward to supporting future reports with IDC insights and analysis within the ever-evolving Kingdom.

CRAWFORD DEL PRETE



*President
IDC*

ACKNOWLEDGEMENTS

This report would not have been possible without the support of IDC's valued partners, the key stakeholders responsible for delivering cutting-edge cybersecurity solutions and services in the Kingdom, and the IDC team that collaborated across different continents, to put together insights and best practices for Saudi Arabia's cybersecurity landscape and use of next-generation technologies.

We are grateful for the support of our sponsors – SITE, Trend Micro, Mobily Business, Cisco and MIS - for sharing their vision and plans to ensure the security of Saudi Arabia's digital transformation efforts.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

1

Saudi Arabia's Cybersecurity Landscape

2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Interview with Al Moammer Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



SAUDI ARABIA'S CYBERSECURITY LANDSCAPE

Overview of the ICT Sector

Saudi Arabia is currently the largest ICT market in the Middle East and Africa (MEA) region. IDC estimates that ICT spending in the region will reach the \$237 billion mark by the end of 2020, growing to \$253 billion by 2023. Saudi Arabia is expected to account for more than 15% of the total regional spending by the end of 2020; in dollar terms, that equates to \$36 billion. Cybersecurity as we know it forms a significant portion of overall ICT spending in Saudi Arabia. IDC research shows that the spending on cybersecurity is expected to reach \$425 million by 2020, and by 2023, it will exceed \$530 million, based on a combined annual growth rate (CAGR) of 6.7% over the five-year forecast period ending in 2023.

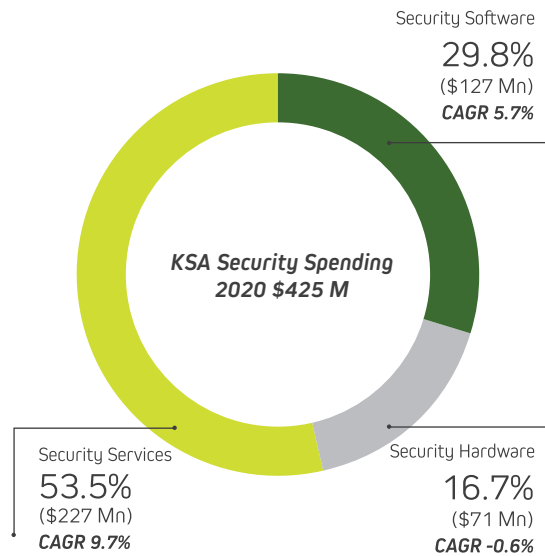
While the cybersecurity market is quite large in itself, key services will drive the majority of this growth. ICT spending in Saudi Arabia has traditionally been product and infrastructure oriented, although growth in those sub-segments is expected to decline. IDC predicts that cybersecurity market growth over the forecast period (and beyond) will be driven by spending on professional services which mainly consist of cybersecurity advisory and consulting, cybersecurity integration and implementation, and managed security services.

The figures below depict spending and growth dynamics of the sub-segments that comprise the cybersecurity market in Saudi Arabia.



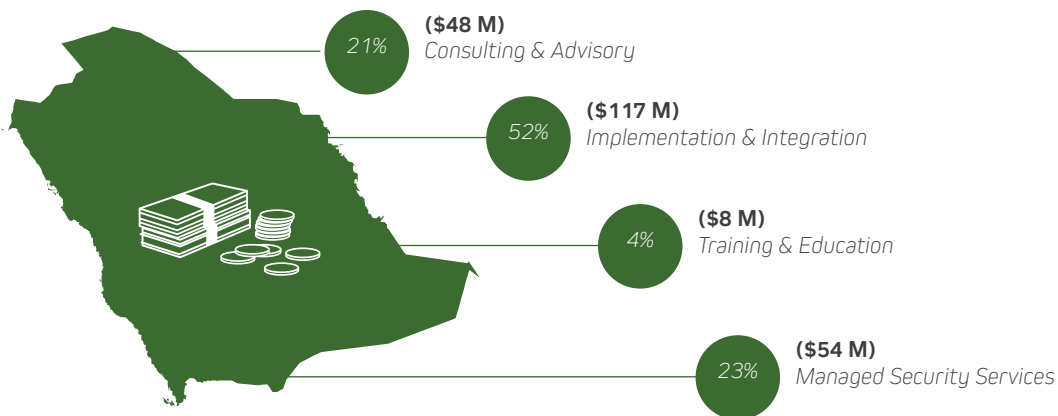
1. Saudi Arabia's Cybersecurity Landscape

FIGURE 1 – SAUDI ARABIA CYBERSECURITY SPENDING BREAKDOWN, 2020 (\$M)



Source:
IDC Security Spending Guide, 2019

FIGURE 2 – SAUDI ARABIA SECURITY PROFESSIONAL SERVICES SPENDING BREAKDOWN, 2020 (\$M)



Source:
IDC Security Spending Guide, 2019

The above figures are a clear indication that Saudi Arabia is moving beyond its infrastructure- and product-centric spending towards more value-added professional services, with the main aim of improving the efficiency of existing infrastructure and applications.

1. Saudi Arabia's Cybersecurity Landscape

Importance of Cybersecurity in the Context of Vision 2030 and the NTP

Although Saudi Arabia's Vision 2030 is expected to create new avenues for economic growth and diversification, the Kingdom continues to be beset by security challenges. In the recent past, Saudi Arabia's critical national infrastructure has been targeted multiple times.¹ These events have played a crucial role in renewing concerns related to cybersecurity in the Kingdom. KSA is determined to improve its cybersecurity posture in the future.

As a result, cybersecurity readiness has become one of the major performance indicators of transformation initiatives across the Kingdom. Saudi Arabia has taken major steps in mitigating future exposure to cyberthreats and is making a concerted effort to fight cybererror. According to IDC's CIO Survey conducted in Saudi Arabia in 2019, 85% of the responding CIOs think that investments in cybersecurity and privacy technologies will be critical to driving digital transformation (DX) initiatives in their organization.

National development plans and diversification initiatives are recognizing emerging technologies as the enablers of pan-industry transformation. That said, adoption of these technologies has exposed both public and private sector organizations to a new wave of cyberthreats. The Kingdom is therefore channeling additional efforts to building capabilities and capacity to secure the technologies enabling diversification initiatives that are the driving force behind the national transformation program. The National Information Security Strategy² (NISS) is among the most important initiatives taken by the Saudi government to formalize the national-level framework for cybersecurity, risk mitigation, and resilience. The draft of this strategy emphasizes the need to improve the Kingdom's overall security and resilience in order to provide a secure foundation upon which a knowledge-based economy can be built.³

While this strategic framework recognizes the need to centralize the management of the local information security environment, including the policies, regulations, and skills required, there is little to no focus on national cybersecurity and critical infrastructure protection (CIP). This is essentially the gap that cybercriminals have tried to exploit in the recent past, thus spurring the development of national cybersecurity and CIP strategies.

1 <https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail>

2 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf

3 https://potomacinstitute.org/images/CRI/CRI2_0_SaudiArabiaProfile.pdf

Centralizing National Security Management

Saudi Arabia plays a crucial role in maintaining security and stability in the region due to its political, economic, and strategic importance. Given the complex and dynamic security challenges facing the Kingdom, especially after recent cyberattacks on high-profile national assets, cybersecurity and cyberdefense have taken on heightened urgency in Saudi Arabia.

In an effort to address these gaps, H.E. King Salman issued a series of royal decrees in 2017. One of the decrees directed the establishment of the National Cybersecurity Authority (NCA) to centralize the national approach to cybersecurity. The NCA has both regulatory and operational functions. The Royal Decree mandates the NCA to develop and oversee the implementation of a national cybersecurity strategy; design cybersecurity governance models, policies, standards, and controls; build a National Cybersecurity Operations Center (nSoC) to execute cyber defense operations; and stimulate the development of human capital and local industry capabilities in the cyber domain, among other tasks.

In 2013 the National Center of Electronic Security (NCES) that reported to the ministry of interior was established. Over the course of time the name of the entity was changed to the National Cybersecurity Center (NCSC) which was repositioned under the leadership of the Presidency of State Security in 2017. The royal decree about the establishment of NCA also directed the repositioning of the National Cyber Security Center (NCSC) to cater to the technical and operational requirements of the NCA.

Saudi Arabia's Improving Image and Influence on the Global Cybersecurity Stage

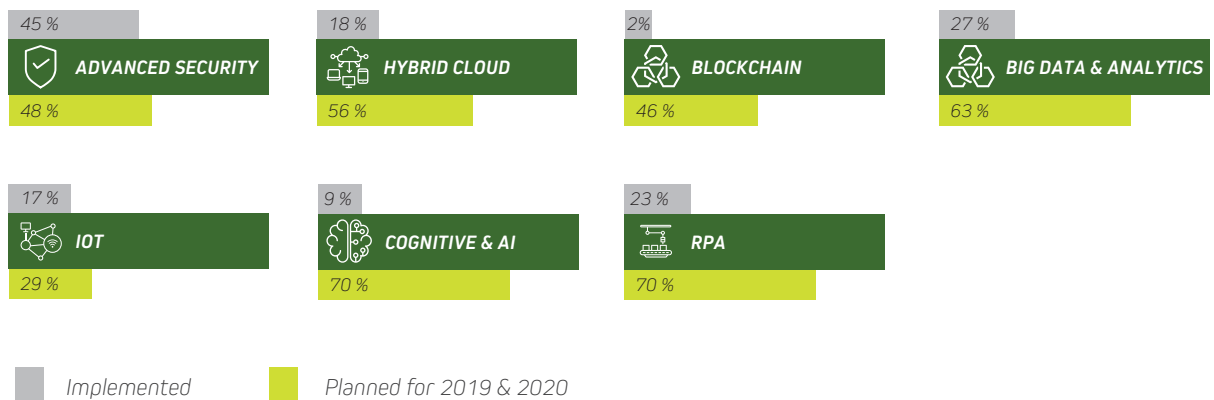
While improving national cyber-readiness and regulating the ICT supply and consumption from a cybersecurity perspective are extremely important, local authorities are also placing significant emphasis on the global perception of Saudi Arabia as a leading contributor to and influencer of cybersecurity development, both locally and globally. In the 2018 edition of the Global Cybersecurity Index (GCI), Saudi Arabia is ranked first across the Arab States and thirteenth globally. The National Cybersecurity Authority has played a vital role in contributing towards these achievements, and through capacity building initiatives and increased collaboration with relevant bodies, aims to improve and consolidate the protection of the Saudi cyberspace and further improve the kingdom's ranking on the index.

Cybersecurity Usage and Adoption Trends in Saudi Arabia

In the past few years, Saudi CIOs have placed increasing focus on information and cybersecurity, particularly as part of their DX agenda. A growing number of high-profile organizations and state assets are being targeted by increasingly complex and persistent cybersecurity threats. Additionally, the push from the Saudi Arabian government to maintain high levels of cybersecurity readiness has encouraged organizations to adopt a more proactive approach to their security posture.

1. Saudi Arabia's Cybersecurity Landscape

FIGURE 3 – EMERGING TECHNOLOGY ADOPTION ROADMAP FOR SAUDI ENTERPRISES



Source: IDC KSA CIO IT Survey, 2019

Innovation Roadmap of the Saudi CIO

The proliferation of 3rd Platform technologies such as cloud, big data and analytics, enterprise mobility, and socially enabled business has drastically increased organizations' attack surface, while innovation accelerators such as IoT, artificial intelligence, and machine learning have further complicated most companies' security posture. This new level of vulnerability has driven the majority of Saudi organizations to reevaluate their approach to security.

Cybersecurity as a Strategic Business Driver

Maintaining the security of digital transformation initiatives is difficult, as most are built on a foundation of 3rd Platform technologies and innovation accelerators. Accordingly, 60%⁴ of CIOs see managing security as the biggest continuing technology-related challenge. This is expected to impact the cybersecurity spending decisions of 46% of Saudi CIOs who have plans to implement advanced security solutions in the coming 1-2 years. Another 75% of CIOs have also placed investments in cybersecurity and privacy technologies as their topmost strategic business objective, especially in view of their digital transformation goals. This is expected to drive overall security spending in Saudi Arabia to \$425 million in 2020, based on a CAGR of 6.7% over the 2018–2023 forecast period.

⁴ IDC's CIO Survey, Saudi Arabia, 2019

1. Saudi Arabia's Cybersecurity Landscape

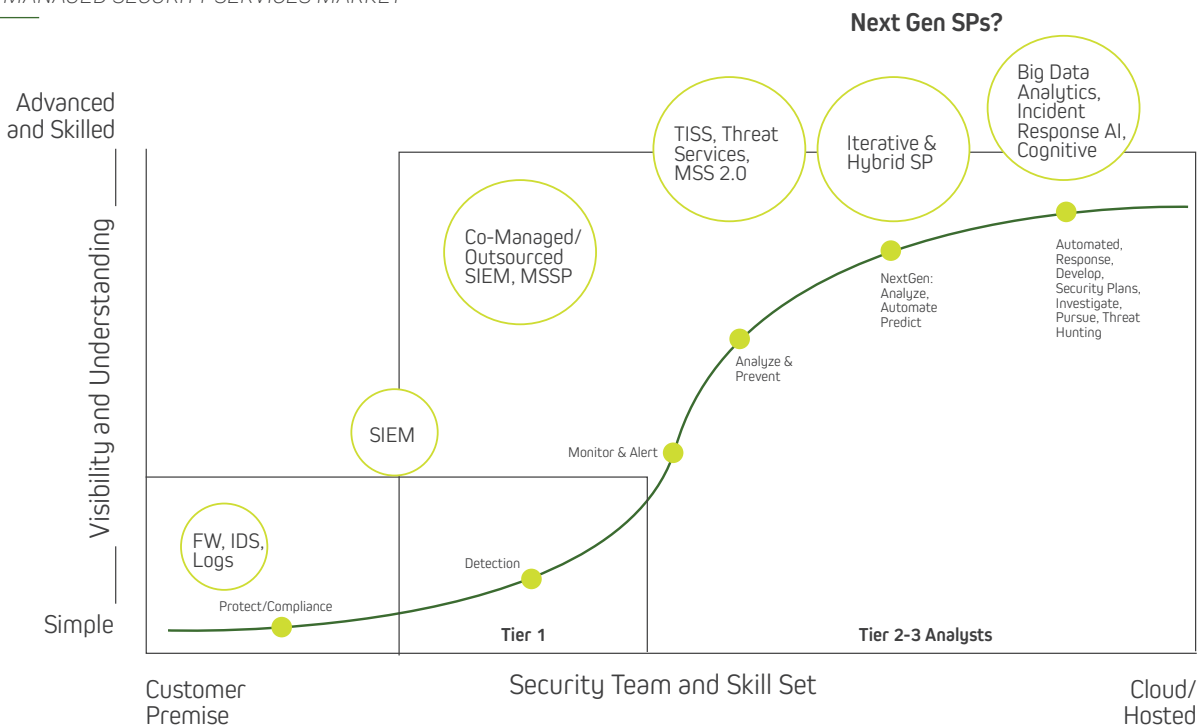
Ecosystem-Based Approach to Cybersecurity

Developing capabilities to manage risk before, during, and after an attack, sharing threat intelligence across the ecosystem, and speeding up response time are major focus areas for Saudi organizations. Committing to the necessary investments, however, requires seeing cybersecurity not as an IT cost, but rather as a key business enabler. Recent developments have necessitated that cybersecurity measures are integrated or built in at all levels of the organization's operations. As a result, service providers and security vendors are actively aligning themselves with customers' business priorities and national-level directives. Providers are also playing a vital role in improving awareness and, subsequently, adoption of advanced security management services such as security operations center (SOC) management, threat intelligence, and advanced detection and analysis. With a view to increasing their levels of service availability, business continuity, and disaster recovery, Saudi organizations are also increasingly relying on third-party specialized cybersecurity firms for advisory, orchestration, and continuous monitoring and improvement-related services.

Automation of Security Management

Security response and incident management is increasingly being augmented by automation through artificial intelligence (AI) and machine learning (ML). While this type of automation may help fortify organizations' cybersecurity postures, false positives associated with use cases have made some organizations cautious about investments. In the long run, widespread automation may eliminate some of the expertise needed to maintain a robust security posture; however, it is also expected to create a pressing need for skills related to supervising AI- and ML-based outputs, and to ensure that automated responses and recovery activities behave more like human intervention.

FIGURE 4 – IDC'S VIEW ON THE EVOLUTION OF THE MANAGED SECURITY SERVICES MARKET



Source: IDC KSA CIO IT Survey, 2019

1. Saudi Arabia's Cybersecurity Landscape

Digital Transformation in Regulated Industries

Cross-industry digital transformation in Saudi Arabia has placed significant pressure on organizations in the healthcare, financial services, manufacturing, and government sectors. Due to the sensitive nature of their operations, organizations in these sectors are expected to maintain the highest levels of cybersecurity. Some high-profile initiatives within the national transformation program include:

Qiddiyah Entertainment City



King Salman Energy City



Integrated Logistics Zone



National Industrial Development Program



Government Procurement and Competition System



1. Saudi Arabia's Cybersecurity Landscape

Healthcare:

Several innovative projects are currently being executed across the healthcare industry, as healthcare development and modernization is a key focus area for Saudi Arabia.⁵ Initiatives that will unify patient data across all healthcare entities using a centralized data exchange platform are driving the Saudi healthcare ecosystem to adopt advanced data privacy and information protection solutions. These investments are helping to increase confidence among patients to let healthcare providers collect, analyze, and use their digital information responsibly to benefit others. Saudi healthcare organizations are expected to place significant emphasis on driving digital trust initiatives⁶ both within the organization and at the national level.

Financial Services:

The Saudi financial services industry is probably the most technologically mature industries in the Kingdom and is undergoing rapid transformation. The need to protect vital customer information and essential operation systems is ongoing, while innovative solutions such as robotic process automation (RPA)-based and AI-augmented have created a new set of information security and data governance challenges. While creating significant efficiencies at the back end, initiatives around automation will put financial services organizations under significant pressure to invest in cybersecurity, with banks and other financial services organizations looking for ways to rationalize their budgets. The Saudi Arabian Monetary Authority (SAMA) has established a cybersecurity framework that is playing a key role in aligning cybersecurity practices within the financial services industry with industry wide standards laid down in the National Cybersecurity Framework for financial services companies.

Cloud Shift and the Matter of Security

As Saudi organizations begin to grasp the potential benefits that cloud computing has to offer, they are rapidly moving more core processes to the cloud, despite initial reluctance to host data and applications outside their internal IT infrastructure. As part of this reluctance was due to the lack of regulations around cloud technology, the Communications and Information Technology Commission (CITC) recognized that legislation was needed for the cloud industry in the Kingdom to grow. For this reason, the CITC's cloud computing regulatory framework emphasizes data classification, especially from a cybersecurity perspective, with customer data classified across four levels of sensitivity that define how the data should be created. In addition, the regulatory framework also has detailed provisions for data residence, breach reporting, data protections, and data infringement. Broadly speaking, these policy changes have certainly improved the appetite for cloud adoption by addressing some of the structural inhibitors such as the lack of a robust classification framework, while promoting fair competition, consumer protection, and regulatory clarity in the cloud market.⁷ As a result, adoption of cloud services increased significantly, as local cloud service providers have actively aligned themselves with the regulation to build local trust. The regulation also provides clarity on the responsibilities of both providers and users of cloud services, which has made international cloud services providers more confident about offering services from their datacenters in the Kingdom. This has also helped address the security considerations of several industries that want to benefit from cloud services but are prohibited from hosting their application and data outside the Kingdom.

⁵ <https://vision2030.gov.sa/en/programs/NTP>

⁶ <https://www.idc.com/getdoc.jsp?containerId=US43986218>

⁷ https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

Security Aspect of Smart Cities and Proliferation of Internet of Things (IoT)

Saudi Arabia has also invested significantly in Smart Cities, with Riyadh aspiring to become one of the leading Smart Cities in the world. However, the Internet of things (IoT) technology that represents the foundation of Smart City processes also presents an attractive target for malicious hackers. Although IoT presents a unique opportunity for service providers in Saudi Arabia, as well as greater efficiencies for end users, lack of properly securing these solutions poses considerable risk to information systems, data, and people. Improperly secured systems can result in significant financial loss, data breaches, health and safety concerns, and threats to national security. Regulators are therefore taking swift action on developing frameworks and mandates that eliminate or significantly reduce cyberexposure across the rapidly expanding attack surface.

Saudi Arabia's CITC drafted regulations and guidance to tackle several topics, including IoT service provisioning, spectrum allocation, IoT equipment and identifiers, data management, and mission critical IoT services. The regulation specifies security and privacy requirements for data management and IoT mission critical services. For example, IoT service delivery infrastructure and the data generated from connected devices must be hosted within the Kingdom's borders. It also mandates applicability of all published laws and regulations relating to data management, including security, privacy, and protection of customer data. These laws, regulations and requirements include the cloud computing regulatory framework published by CITC. Regarding critical IoT services, the cybersecurity requirements for providers are necessarily higher, since failure of such services could result in a serious impact on health, public safety, resources, or national security.⁸

⁸ https://www.citc.gov.sa/en/new/publicConsultation/Documents/144004_2.pdf

2

Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape

3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape

DR. SAAD S. ALABOODI

CEO and Board Member, Saudi Information Technology Company (SITE)



Dr. Saad Alaboodi is the CEO and board member of Saudi Information Technology Company (SITE). He is an accomplished and highly driven entrepreneur, with a proven experience of over 20 years in the technology industry. Dr. Alaboodi has worked in various positions in private domestic and international companies and has extensive expertise in dependability, and cybersecurity fields. He was an assistant professor at the College of Computer and Information Sciences at King Saud University.

Dr. Alaboodi is a result-oriented, decisive and visionary team builder, and leader in new market identification and strategic positioning for multimillion-dollar digital and cyberorganizations.

He excels in dynamic markets and demanding environments while remaining pragmatic and focused on realizing vision and objectives.

Dr. Alaboodi has extensive knowledge of current economic, social, and regulatory issues related to digital and cyber environments and holds the following qualifications:

- PhD in Computer Engineering, University of Waterloo.
- Master of Applied Science (MAsc) in Computer Engineering, University of Waterloo.
- Master of Business Administration (MBA), University of Hull.
- B.Sc. in Information Systems, King Saud University.

2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape

Q1. How would you describe, in a few sentences, the importance of cybersecurity in the context of the ongoing digital transformation, especially with the growing sophistication of cyberthreats?

Historically, Digital Transformation revolves around the abundance of opportunities it introduces in our societies, including boosting efficiency and productivity. But today, the notion expanded into two areas; the opportunities it creates, and the unprecedented threats it simultaneously introduces. The challenge becomes not only about what we want to do, but also what we do not want to happen. This has made security in the digital age a critical factor in everything we do—today, we call this Cybersecurity. Consequently, reliability and confidence in technology adoption has shifted to multiple levels: confidence in the privacy of Personally Identifiable Information (PII), confidence in the security of critical information in digital form and digital transactions, and confidence that natural and/or manmade (or stimulated) events will not disrupt any aspect of human lives and the nations' critical infrastructures.

Q2. With the public sector at the helm of digital transformation in the Kingdom, what is your view on the various initiatives that the Saudi government has launched in order to improve the local cybersecurity landscape?

The boldest and most proactive step taken by the Saudi government is its unique two-front initiative to establish cybersecurity as a new industry in the Kingdom. On the one hand we have the establishment of the National Cybersecurity Authority (NCA), the central government authority responsible for cybersecurity in the Kingdom and its agenda, strategy, and regulations. And on the other we have the establishment of a commercial entity, Saudi Information Technology Company (SITE), to serve as the technical and operational arm of the NCA in this domain. SITE's vision and strategy is centered on enabling secure digital transformation

of both public and private sector organizations, and supporting the development of cybersecurity as a vibrant industry within the Kingdom. Together, the NCA and SITE, form a full-spectrum partnership within Saudi Arabia and with international partners in the global cybersecurity arena.

Q3. What are some of the key activities your organization has undertaken to enable the government's vision to strengthen Saudi Arabia's cybersecurity outlook?

As the technical and operational arm, SITE supports the NCA in fulfilling its responsibilities and addressing the cybersecurity needs of the government, Critical National Infrastructure, and the private sector by providing two distinctive offerings: The first is what I would call a Diagnosis offering, which is centered on a complete portfolio of cybersecurity solutions and services. This offering covers the full spectrum of cyber from proactive to reactive—think of these as protecting and defending the enterprise and responding to events within it. The second is a Resolution offering, which is centered on enabling the secure digital transformation journey through design, development, and monitoring of secure-by-design enterprise solutions, augmented with tailored cybersecurity and digital human capital development programs to build a pool of highly qualified Saudi talents.

In collaboration with the NCA in fulfilling our mandates, and in just about three years, SITE has served public and private sector organizations, supporting them in becoming more resilient in the face of cyber challenges. On this note, and although SITE's achievements are important, it is how we achieved them is paramount to us. The majority of our delivery has been conducted through our local, highly talented, and gender-diverse workforce of which more than 80% are technical employees and 28% are females. Of course, we can never fulfill our potential if we walk alone, to this end, and in parallel to the 'home grown' approach, we continue to develop strategic, sustainable partnerships to accelerate capability development and expand

2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape

delivery capacity. SITE continually looks across the globe for best-of-breed companies that share the mission focus, high technical and ethical standards and philosophy with whom SITE can establish long-term, mutually beneficial relationships. The overall result translates directly into increasing the Local Technical Content in this domain.

Q4. IDC research shows that managing enterprise security is the biggest technology-related challenge for CIOs today. What challenges do you see arising as innovative technologies (like IoT, cloud, artificial intelligence, etc.) drive digital transformation initiatives?

Similar to the convergence between physical and technical security a few years ago, I believe today we are witnessing another important convergence of ICT and ICS technologies into the same ecosystem, and how IoT and ubiquitous devices and technologies can inadvertently and reliably bridge these environments. CIOs now have to be knowledgeable of how threats to each of these environments can traverse from one to the other, the issues related to supply chain security, including the update and sustainment of technology products. They also need to deal with the impact beyond hardware and software integration, which is the evolving local and international policy and regulatory environments concerning these new technologies.

Q5. How prepared is the Kingdom when it comes to securing these technologies?

Like many countries worldwide, Saudi Arabia has

made significant progress in addressing these challenges, but cybersecurity is a continuous journey, not a destination. Pressure to physically redistribute and move data away from data owners due to the emergence of new computing paradigms like Cloud, Edge, and Ubiquitous Computing, acceleration of remote work models adoption, the pace of technology change (5G, IoTs, Artificial Intelligence/Machine Learning), and the growing availability of offensive tools to anyone with a computer and an Internet connection means that we, like all other nations, will always be working to maintain the resilience of the Saudi digital ecosystem in order to advance technology adoption, safeguard our digital assets, and contribute to the cyber resilience at the global stage.

Q6. What would be key advice for the government to catapult the Saudi cybersecurity ecosystem further into the future?

The establishment of the National Cybersecurity Authority and SITE were foresighted moves by the Kingdom. Establishing a comprehensive policy and regulatory framework to govern the use of Saudi digital infrastructures, sharing threat information with international entities, and adopting cyber initiatives and partnering with cybersecurity companies globally are all steps to continuously enhance the resilience of the cyberspace both locally and globally. The focus on developing a critical mass of capable cybersecurity professionals in the Kingdom will ensure the Kingdom's continued progress and contribution to the global cybersecurity stage.

1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape

3

Evolving Competitiveness of the Local Cybersecurity Ecosystem

4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



Evolving Competitiveness of the Local Cybersecurity Ecosystem

Developing Skills and Building Capacity around Cybersecurity

The Kingdom has suffered from a scarcity of advanced IT skills in the field of cybersecurity for a considerable amount of time. Given the pace of global technology innovation, including on the cybersecurity front, skills required to run and operate advanced cybersecurity tools and controls are not easy to onboard and retain. Moreover, technology skills are becoming obsolete at an increasingly rapid rate. As a result, the skills gap in Saudi Arabia has been continuously widening. However, over the past few years, Saudi Arabia has launched a variety of programs to address IT and cybersecurity skills shortage. In addition to granting 231 scholarships to students that choose to specialize in cybersecurity, the Kingdom trained 751 employees from 113 companies and 288 students on cybersecurity protocols. The Saudi Research and Innovation Network (Maeen) was established in 2017 to advise Saudi organizations on regulatory compliance, information security recommendations, and cyberattack investigations.⁹

State Sponsored Cybersecurity Education and Training Programs

Several government authorities are signing partnerships and memoranda of understanding in this regard. For instance, in February 2020, the Human Resource Development Fund (HRDF) of Saudi Arabia signed an agreement with the National Cybersecurity Authority (NCA) to train Saudi nationals in the field of cybersecurity and qualify them for jobs in the private sector. Under HRDF's Daroob program for training and qualifications, the main aim of the partnership is to equip the Saudi workforce with skills, knowledge, and professional capabilities necessary to succeed in the cybersecurity landscape.

The Public Investment Fund (PIF) backed NEOM has also signed agreements with the NCA and several other educational institutions such as Prince Muqrin bin Abdulaziz University and the University of Tabuk to train hundreds of students in cybersecurity.¹⁰ Announced in November 2019, the Saudi Arabian Monetary Agency also launched its third iteration of its specialized program in cybersecurity. SAMA launched Secure 19, a 20-week program to train and qualify Saudi resources in to work in cybersecurity. The trainees will receive technical training and practical application perspectives by specialized international experts on topics such as defense, protection, governance, infrastructure, and attack and penetration testing.¹¹

Development of human capital with respect to the field of cybersecurity is a key strategic imperative in the national information security strategy that aims at expanding the capability of Saudi information security practitioners, researchers, and entrepreneurs, and promoting cybersecurity training and awareness. In order to further propel human capital development in Saudi Arabia, the MCIT launched talent development programs and partnerships with global IT companies to train over 56,000 Saudi youths on key ICT skills between 2017 and 2020. MCIT also established a National Information Technology Academy in collaboration with Saudi Aramco to train and develop Saudi talent. The NISS proposes a program beginning in primary school that encourages children to acquire computer, analytical, and cyber security skills from an early age in a hope to protect the Kingdom's cyber-future.

⁹ <https://us-sabc.org/saudi-arabias-emergence-in-cyber-technology/>

¹⁰ <https://www.constructionweekonline.com/products-and-services/262836-neom-as-a-smart-city-goes-beyond-traditional-security-systems>

¹¹ <http://www.sama.gov.sa/en-US/News/Pages/news20112019.aspx>

3. Evolving Competitiveness of the Local Cybersecurity Ecosystem

Academic Focus on Cybersecurity Capability Development

The Kingdom also established the Prince Mohammed bin Salman (MBS) College of Cyber Security, Artificial Intelligence and Advanced Technologies. In 2018, the college signed a partnership agreement with IronNet Cybersecurity, a US-based cybersecurity company to benefit from the experience of senior cybersecurity advisors from the Cyber Command of the US Department of Defense. The MBS College of Cyber Security, Artificial Intelligence and Advanced Technologies thus became the first educational institution in the region to offer specialized educational programs in cyberwarfare.¹²

Increasing Global Cooperation in the Field of Cybersecurity

Over the last two years, several entities in Saudi Arabia have signed international agreements and memoranda related to cybersecurity. In April 2019, the NCA signed an agreement with the World Economic Forum (WEF) to build a resilient and secure cyberspace that protects national and citizens' interests, while fostering Saudi Arabia's economic growth. More recently in February 2020, the NCA also signed an agreement of cooperation with Underwriters Laboratories (UL), a global safety certification company to defend the Kingdom against cyber threats by developing a national framework for cybersecurity according to the highest international standards.

In early 2020, the Misk Initiatives Center in Saudi Arabia signed a memorandum of understanding with the University of Tokyo to set up the Mohammed bin Salman Center for Future Science and Technology in the university. The MoU will focus primarily on scientific and technology R&D in fields of big data, cybersecurity, energy, mechatronics, robotics, and medical and biological sciences to support the admission of Saudi scholarship students into academic and research programs at the University of Tokyo. In 2019 alone, the Misk Initiatives Center signed 12 MoUs with local and international organizations such as Huawei, Total, the Emirati Federal Youth Authority, and the Ministry of Economy and Planning to support and develop young talent.

Entrepreneurial Focus on Cybersecurity

In order to build local competencies and bring cybersecurity into entrepreneurial focus, Saudi Arabia is extensively funding R&D and investing capital into promising local and global cybersecurity start-ups. In December 2019, the Riyadh Valley Company (RVC) participated in round-B investment in SecuLetter, a South Korea-based cybersecurity startup. This investment will let SecuLetter strengthen its R&D and enhance its products. RVC was established in 2010 as an investment arm of King Saud University specifically focusing on acquisitions, mergers, and alliances, in addition to holding strategic partnerships with all governmental and private bodies, local and global, that will support enriching and diversifying the KSA economy.¹³

Growing Regulatory Maturity and New Ecosystem Stakeholders

Saudi authorities are developing the local cybersecurity landscape by establishing new frameworks and policies, some of which have created upheaval in the local market, particularly industry-specific regulations such as SAMA Cybersecurity Framework for the finance sector. Nevertheless, the cumulative effect of

¹² <http://english.alarabiya.net/en/business/technology/2018/07/04/Mohammed-bin-Salman-Cyber-Security-College-signs-deal-with-IronNet-Cybersecurity.html>

¹³ <http://rvc.com.sa/?p=1863&lang=en>

3. Evolving Competitiveness of the Local Cybersecurity Ecosystem

these regulations has been to increase end user confidence, and organizations are more readily investing in cybersecurity services and aligning their internal policies on cybersecurity and data governance with those of market and government regulators.

SAMA's Cybersecurity Framework

Improving resilience to cyberthreats is a strategic business priority for financial services organizations. Given the sensitivity of the data and the value of the transactions conducted in the Saudi financial services domain, SAMA released a cybersecurity framework in May 2017 that helps regulated financial entities to identify and address cyber security risks. All banks, insurance companies, and finance companies operating in the Kingdom are required to comply with SAMA's regulations. The framework also applies to subsidiaries and the personnel of such entities, as well as to third party contractors and customers.

SAMA examined global industry standard frameworks that were adapted for the local framework to ensure that the regulation is robust and all inclusive. These frameworks include:

- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO 27001/27002 Information Security Management Standards
- Information Security Forum Standard of Good Practice for Information Security
- Basel II International Convergence of Capital Measurement and Capital Standards

The framework has been developed on the basic premises of confidentiality, integrity, and availability and prescribes key cybersecurity principles and objectives to be achieved by each regulated entity across four cyber security domains:

- **Leadership & Governance:** The framework requires having a board-endorsed, committee-led cybersecurity governance structure. Organizations must establish a cybersecurity function separate from the IT department, preferably led by a Saudi CISO.
- **Risk Management & Compliance:** Regulated entities must conduct risk identification, analysis, response, monitoring, and review of their cybersecurity controls at regular intervals under a defined and approved cybersecurity risk management process.
- **Operations & Technology:** Regulated entities must ensure that their information assets are secured with appropriate controls and conduct regular cybersecurity awareness training. The framework also provides guidelines around bring your own device (BYOD) policies.
- **Third Party Considerations:** Regulated entities must adhere to the framework guidelines even when dealing with third parties such as information services, outsourcing, cloud service providers, technology providers, and governmental agencies.

CITC Cybersecurity Regulatory Framework (CRF)

In 2019, the CITC released the Cybersecurity Regulatory Framework (CRF), which aims at providing better management of cybersecurity risks through a consistent approach aligned with international best practices and local cybersecurity dynamics. Key objectives of the framework include regulating cybersecurity practices in the Saudi ICT sector, increasing cybersecurity maturity, inculcating a risk-oriented approach to

3. Evolving Competitiveness of the Local Cybersecurity Ecosystem

cybersecurity while ensuring confidentiality, integrity, and availability of the e-government services provided to citizens, residents, and businesses. The CRF also clarifies the minimum security requirements for licensed service providers. In order to ensure the readiness and maturity of cybersecurity service providers, the framework also regulates governance, asset management, risk management, internal security, and third-party security. Each of the articles mentioned in the regulation has a list of necessary controls that are mandatory for compliance with the framework.¹⁴

National Cybersecurity Authority's Essential Cybersecurity Controls

In 2017, a royal decree was also released that approved the regulation of the NCA and set out their role and responsibilities, which include:¹⁵

- Developing and implementing the national cybersecurity strategy
- Creation of policies, frameworks, and standards for different aspects of cybersecurity (implementation, risk management, incident response, encryption, etc.)
- Establishing and operating national platforms and operations centers with command, control, investigate, monitor, and information exchange and analysis capabilities

In 2018, the NCA issued guidelines in the form of Essential Cybersecurity Controls (ECC). These are minimum cybersecurity requirements for all public and private sector entities that either own, operate, or host critical national infrastructure (CNI). The ECC consists of 114 cybersecurity controls that take local and international regulatory requirements into account and are structured into five main domains:

- **Cybersecurity Governance:** Envisions the development and implementation of a cybersecurity strategy that contributes to compliance with relevant laws and regulations. The strategy should clearly stipulate personnel, processes, roles and responsibilities, policies and procedures, risk management, review policies, response protocols, and awareness and training provisions needed to achieve effective cybersecurity.
- **Cybersecurity Defense:** Organizations subject to the ECCs should have physical security and other measures to protect information and technology assets from threats. Data and information are to be classified in line with regulations. Encryption, back-up and recovery, security log analysis, and incident management systems must be in place.
- **Cybersecurity Resilience:** This covers incorporating cybersecurity resiliency requirements into business continuity processes, in order to reduce the impact of cybersecurity incidents on systems, data processing facilities, and critical services.
- **Third-Party and Cloud Computing Cybersecurity:** Requires controls to mitigate third-party risks associated with outsourcing and managed services in compliance with organizational policies and procedures. Protecting data and infrastructure hosted in the cloud is also critical; datacenters must be located in the Kingdom.
- **Industrial Control System Cybersecurity:** Industrial control systems must be managed appropriately to protect the confidentiality, integrity, and availability of their assets against unauthorized access and destruction.

¹⁴ https://www.citc.gov.sa/en/new/publicConsultation/Documents/144010_1_E.pdf

¹⁵ <https://www.tamimi.com/law-update-articles/cyberabia-developments-in-the-cybersecurity-regulatory-landscape-in-saudi-arabia/>

3. Evolving Competitiveness of the Local Cybersecurity Ecosystem

CERT-SA's Information Security Policies and Procedures Development Framework for Government Agencies

In 2010, CERT.sa (Computer Emergency Response Team – Saudi Arabia) also released the Information Security Policies and Procedures Development Framework for Government Agencies to expand its statutory responsibilities under the Council of Ministers Act, that assigns CITC and CERT.sa to develop and propagate information security policies and guidelines, including minimum requirements to help Saudi government agencies ensure effective management of information security risks. The framework discusses the fundamental elements required for developing and maintaining information security policies and procedures together with standardized documents and the accompanying development processes. This framework aims at helping local government agencies standardize and develop their information security policies and procedures. While the framework is intended for government agencies: It can also be used by other public and private sector organizations in Saudi Arabia and abroad.¹⁶

In 2017, the royal decree that directed the formation of the NCA, also mandated the transfer the Computer Emergency Response Team (CERT) from the Communications and Information Technology Commission (CITC) to the NCA.

International Cybersecurity Forums Find a New Home in Saudi Arabia

Saudi Arabia is fast becoming the hot spot for regional and global cybersecurity conferences and summits, where international experts and companies specialized in cybersecurity converge to discuss strategy, compliance, legislation, governance, and the importance of integrating cyber-awareness into corporate culture. In February 2020, the first Global Cybersecurity Forum was held in Riyadh, which provided a platform for several announcements that will contribute to the global cybersecurity posture. Initiatives such as Protection of Children in Cyberspace, aimed at creating a safe cyberspace for children and protecting them against cyber-bullying and aggression and Empowerment of Women in Cybersecurity, to enable women to work in cybersecurity positions, while increasing women's participation and contribution to cybersecurity globally were launched at this forum. The General Department of Cybersecurity at King Khalid University was one of the first movers in this space in Saudi Arabia, aspiring to increase the percentage of women working in the field of information and cybersecurity.

¹⁶ https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/CITC_Information_Security_Policies_and_Procedures_Guide_En.pdf

1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem

4

Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Interview with Al Moammār Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

DR. MOATAZ BINALI

Vice President, Trend Micro Middle East & North Africa



As Vice President for Trend Micro Middle East and North Africa (MENA), Dr. Moataz Binali is responsible for spearheading the company's strategy across the region, and advancing its position as a leader in cybersecurity that is passionate to make the world safe for exchanging digital information.

A significant part of Dr. Binali's role is to oversee Trend Micro's efforts in enhancing the cybersecurity posture amongst governments and enterprises, contributing to the digital economy of MENA. His leadership has been instrumental in establishing long term partnerships in both public and private

sectors, as well as growing the company's footprint, and channel partner ecosystem by bringing the technical expertise and business resources.

Dr. Binali is a technology expert with over 20 years of experience in the IT industry. Prior to joining Trend Micro, Dr. Moataz Binali has held pivotal roles on regional level in global technology organizations such as SAP, IBM, and Microsoft. He has a Doctorate in Technology Innovation Management, a Master certificate in System Design & Project Leadership, and an OM-MBA in Organizational Management. His bachelor's degree was obtained in Software Engineering.

4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

Q1. How would you describe, in a few sentences, the importance of cybersecurity in the context of the ongoing digital transformation, especially with the growing sophistication of cyberthreats?

As governments and organizations in the region pursue their digital transformation ambitions by adopting emerging technologies, cybersecurity has become a key pillar in this journey – a landscape that evolves every day, and keeping up with its unprecedented speed remains a challenge for many. Newer and more sophisticated attacks surface each day – from malware, spyware and ransomware to phishing practices, and from network compromise, data center compromise, email compromise, to crypto mining and many more.

Our 2019 Security Round up report found that malware attacks were one of the biggest cyber threats with a total of 5.54 million in the GCC – making it the fifth most-hit region by malware in Asia, and 14th in the world. Countries that endured the most attacks were Saudi Arabia (2.35 million) and the UAE (1.98 million).

Additionally, in the first quarter of 2020 year alone, Trend Micro detected and blocked 9,773 COVID related threats in the GCC. Email spams were the highest (8,984) the 4th highest in Asia, followed by URL attacks (772) and malware (17). Globally, we have seen a 220x times increase in COVID related spam between February and March of this year.

The evolving threats and staggered findings give out a clear message – that organizations need resilience to stay ahead of these threats. To that end, Trend Micro delivers a unique approach of what we call - *The Art of Cyber Security*. Our commitment to bring smart, optimized, and connected technology is at the heart of our mission of making the world safe for exchanging digital transformation and empowering organizations to prepare for, withstand, and rapidly recover from threats.

Q2. With the public sector at the helm of digital transformation in the Kingdom, what is your view on the various initiatives that the Saudi government has launched in order to improve the local cybersecurity landscape?

The Government of Saudi Arabia is amongst the leaders in the region in its tireless efforts towards addressing cybersecurity - a key pillar of its Vision 2030 to digital infrastructure development. Establishment of the Saudi National Cybersecurity Authority (NCA) and digital initiatives like the 'attaa' are at the heart of the government's strategy to protect our society from cyber-attacks.

Driven by the country's strong leadership, the NCA has built strong partnerships with global technology players and private organizations to accelerate innovation and investments in cyber security – contributing to a secure future of the Kingdom's economy.

Q3. What are some of the key activities your organization has undertaken to enable the government's vision to strengthen Saudi Arabia's cybersecurity outlook?

Trend Micro has established a strong presence in Saudi Arabia with our MENA headquarters based here in Riyadh, and we are working across many facets to support the government's vision. We have invested considerably in the ecosystem at large by working closely with the public and private sectors, building the capacity of our partners, bringing technology transfer, as well as training and development of cybersecurity professionals. Some of our efforts include:

- Trend Micro signed a **Managed Services Partner (MSP)** agreement with **the Saudi Telecom Company (STC)** to better secure cloud journeys of organizations in Saudi Arabia.
- We have also been resilient in our commitment to the country's startup ecosystem. As part of the **Trend Micro 'Start Safe Program'**, we aim to support **1000 Saudi start-ups** with a co-funded

4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

cybersecurity platform to help them focus on their core business, grow with our protection, and build the right community around them.

- We partnered with **CyberX**, a program under the umbrella of “Attāa initiative” to protect the society from evolving attacks. This effort is part of our global Initiatives for Education that supports Internet safety for kids and families, small businesses, and universities. As part of the same effort we also partnered with the “**CyberKids**” association to raise awareness and help mitigate online risks as well as teach good digital citizenship.
- Last year, Trend Micro also partnered with the Saudi education-technology company **TETCO** in an initiative to unify security measures across 28 universities and more than 30,000 schools in the kingdom.
- Through our Saudi Academy for Cyber Security, we are strengthening the capacity of young graduates to nurture their skills in cyber security and develop them into industry leaders. We have also entered into an academic alliance with the **Naif Arab University for Security Sciences (NAUSS)** to support in developing cyber security courses for regional security leaders as well as conduct a comprehensive ‘train the trainer’ program for select university faculty in cyber security courses.
- Also, we are a strategic partner with **Cyber Talents** to host the Arab Regional **Cybersecurity CTF (Capture the Flag)** competitions every year to nurture the youth. Last year, 3 winning teams from Saudi Arabia qualified to participate in the global challenge.

Q4. IDC research shows that managing enterprise security is the biggest technology-related challenge for CIOs today. What challenges do you see arising as innovative technologies (like IoT, cloud, artificial intelligence, etc.) drive digital transformation initiatives?

Cloud services have become the cornerstone of digital transformation for many governments and

organizations in the region, and technologies such as AI and IoT are fueling this journey.

Indeed, this opens doors to many vulnerabilities from a security perspective. Whether it’s misconfigurations in the cloud or gaps in the networks – the growing connected devices, endpoints and sensors, remote working threats, or the rising skills gap - today’s CIOs will have to holistically address these challenges to manage this risk before, during, and after an attack in our increasingly connected world.

Detection and response are a vital security requirement for all organizations. **Trend Micro XDR** extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With XDR, our customers can respond more effectively to threats, minimizing the severity and scope of a breach.

Along with Cloud migration, one needs additional protection for what one puts IN the cloud – workloads, apps etc. To this end, **Trend Micro Deep Security, powered by XGen security** uses a blend of cross-generational threat defense techniques to protect cloud workloads from breaches and accelerates compliance with all standards. Our cloud security offerings integrate perfectly with all cloud providers including AWS and Azure.

It is also imperative for organizations to take a modern and layered approach to security. Solutions such as Trend Micro’s **Connected Threat Defense** help businesses quickly protect, detect, and respond to new threats while simultaneously improving visibility and streamlining investigation across your entire IT infrastructure.

Our innovations are built from the ground up to empower CIOs and security professionals in their journey of protecting their organizations from the endpoint – to the cloud. Trend Micro has created an integration architecture, enabling endpoints, networks, virtual servers, and cloud and container-based workloads to work together for enhanced visibility and coordinated threat response. This empowers our customers to innovate freely while leaving their security to us.

4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

Q5. How prepared is the Kingdom when it comes to securing these technologies?

Saudi Arabia is taking leaps in its approach to improve the country's cyber security posture. The efforts by the NCA, the Federation for Cybersecurity, Programming and Drones, and the Ministry of Communications and Information Technology - are all steered towards the vision of a secured digital future of public and private organizations, as well as individuals. Trend Micro shares this vision with the government by working closely across public and private organizations to enable them in this journey.

Our strategy in Saudi Arabia centers on 3Cs - (**"committed"**, **"connected"**, **"complete"**). The **Commitment** we bring to the Kingdom is distinct from that of other vendors with our strong local presence to offer technical expertise and business resources. **Connected** comes from the power of our connected threat defense across all layers and bringing them together. **Complete** denotes our holistic cybersecurity solutions portfolio that addresses the defense and protection needs across endpoints, hybrid cloud and networks.

Our end goal is to become a trusted partner of choice to the Saudi government and the private sector, and we are working towards this by bringing the right technology and expertise to the Saudi market. Just recently Trend Micro was named Google Cloud's 2019 Global Technology Partner of the Year for Security. Forrester has also ranked us as a leader in their Forrester Wave™: Cloud

Workload Security report for Q4 of 2019. We received the highest score in the categories of current offering and strategy.

Additionally, IDC recognized and named Trend Micro as the #1 vendor in Software-Defined Compute (SDC) workload protection. The report also revealed that we achieved a market share lead of 35.5%, almost 3 times our nearest competitor in 2018.

These achievements speak clearly about our efforts of delivering innovative solutions to meet the ever-evolving threat landscape and the needs of our customers.

Q6. What would be key advice for the government to catapult the Saudi cybersecurity ecosystem further into the future?

The government is headed in the right direction by taking strong awareness and policy measures to protect our society from cyber-attacks as well as working tirelessly to enable new Saudi talent in the cyber security field. From a technology perspective, adopting a multi-layered approach to security is critically vital considering how rapidly the landscape is evolving and this is one of the key areas that we're working on in partnership with the government.

With our commitment to the country and the whole region, we see our role as more than just a security vendor - rather a partner that aims to play a critical role in the progress of Saudi Arabia's digital economy and its IT Ecosystem.



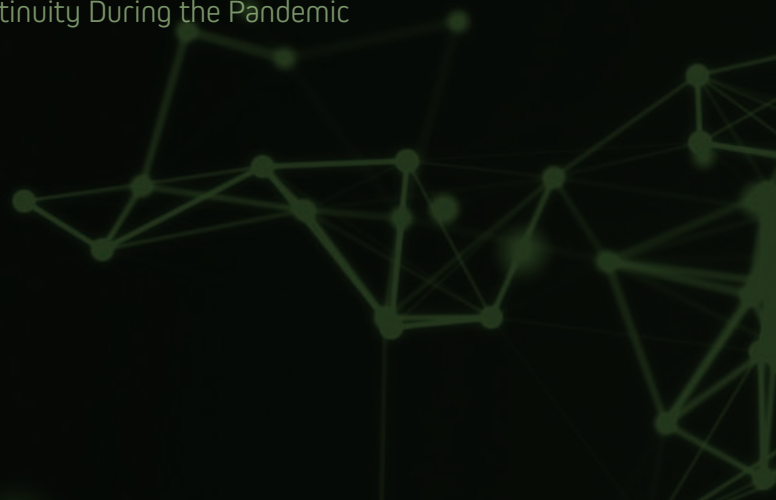
001
1110
0101
0001
00010
1000
0101
1111
1111

1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape

5

Initiatives & Developments to Improve the Saudi Cybersecurity Environment

6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Interview with Al Moammar Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment

INITIATIVES & DEVELOPMENTS TO IMPROVE THE SAUDI CYBERSECURITY ENVIRONMENT

As Saudi Arabia moves towards the localization of content and services in line with Vision 2030, the cybersecurity landscape has undergone significant evolution. Saudi Arabia has become a major target of cyber conflicts, due to increased economic activity, ongoing digital transformation initiatives, and increased technology adoption among consumers and businesses. The Kingdom's geopolitical position and natural resources have also made it a lucrative target for cyberattacks, especially in regard to the oil & gas and petrochemicals industry.

Realizing the Need for a Policy Driven Approach

Although Saudi Arabia was ranked 13th globally and 1st in the Arab world in the Global Cybersecurity Index published in 2018, local businesses are concerned about security. Rightfully so, as Saudi Arabia ranks second in the cost of data breaches and much higher than the global average of compromised records per breach, at 38,800 (compared to 25,575).¹⁷ Certain attacks in the last decade have made the importance of cybersecurity clear and forced Saudi organizations to increase investments in cybersecurity innovation. As a result of national transformation initiatives in the Kingdom, even the ministries and regulators have realized the importance of cybersecurity for the economy, and outcomes for citizens, and enterprises. Relevant stakeholders have worked towards building the legislative and regulatory framework for cybersecurity oversight in Saudi Arabia. Although existing legislation such as the Anti Cyber Crime Law for investigating and prosecuting cybercrimes and the Electronic Commerce Law to curb online fraud provide some recourse against cyber miscreants, the kingdom has realized the need to create robust guidelines to regulate the local cybersecurity, with a unified strategy already underway.

Saudi Arabia has been strengthening the legislative foundation required to regulate emerging technology markets, with considerable emphasis on security. CITC's Cloud regulations, SAMA's cybersecurity principles, and NCA's Essential Cybersecurity Controls all have cybersecurity at their core. Even the latest IoT Regulations recently published by CITC emphasizes the security aspect of IoT adoption and usage. In addition, the government has already established national-level governing bodies and regulators such as the NCA whose role in the coming years will only become more pronounced as they start enforcing the mandates under their purview.

¹⁷ <https://www.cio.com/article/3445225/saudi-arabias-cybersecurity-concerns-increase-as-threats-evolve.html>

5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment

Saudi Arabia Becoming a Lucrative Target for Cyber Adversaries

Not surprisingly, Saudi Arabia is the target for the highest number of cyberattacks in the Middle East. An estimated 60 million attacks daily target public and private sector organizations with the aim of destabilizing the economy.¹⁸ Although there are large-scale transformation initiatives ongoing across industries, a report by the Global Foundation for Cyber Studies and Research has identified a lack of local training courses and general unawareness of the dangers posed by cyberattacks as the main sources of vulnerability.

Strategic Nature of Motivations Behind a Cyberattack

While a lot is being done to fortify the competitiveness of the local cybersecurity ecosystem, cybermiscreants are on a relentless drive to innovate in parallel. The cyberattacks we see today have evolved from the basic threats of previous years. As threats continue to evolve and become more persistent and targeted, critical national infrastructure has become more exposed.¹⁹ In December 2019, Saudi authorities discovered a new variant of data-wiping malware that suggests the work of state-sponsored hackers. However, the damage was limited compared to previous years, due to early discovery of the attack, aided by the NCA. Cybersecurity analysts in the US Department of Homeland Security have observed a growing trend where state-sponsored cybercriminals are increasingly using data wipes or exfiltration to gain a better understanding of national strategic direction and policymaking of the target country.²⁰

Cybercriminals Increasingly Targeting the Public

Accelerated digital transformation and inadequate cybersecurity measures in key sectors, along with poor security habits of end users, have made Saudi Arabia a cyber target in the past. Some of the most rampant attack vectors that constantly threaten the national cybersecurity include:

- Botnets typically used to spread malware and spam across company networks are on the rise. With 11.4% of the Middle East's bot population residing in the GCC, Saudi Arabia alone accounts for more than 43% of these bots.
- Social engineering is another sophisticated attack vector that has been increasing in Saudi Arabia in recent years, with cybercriminals deceiving individuals into divulging credentials that may be used for hacking or to perpetrate fraud.
- Although identity theft is not currently a major concern in Saudi Arabia, the growing trend may give rise to an economy that is fueled by stolen identities. Globally, stolen identities have been used to conduct financial fraud going all the way into conducting acts of terrorism under aliases (stolen identities).

18 <http://english.alarabiya.net/en/media/digital/2017/05/02/60-million-cyber-attacks-targeted-Saudi-Arabia-in-one-year.html>

19 <https://aawsat.com/english/home/article/1557001/cyber-security-fastest-growing-sector-saudi-arabia>

20 <https://www.cyberscoop.com/saudi-arabia-iran-cyberattack-soleimani/>

5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment

Cyberattacks Posing an Increasing Threat to Human Life

The risk of cyberattacks is no longer limited to business and data. As IT and operational technology (OT) merge, developing a holistic approach to maintaining high levels of cybersecurity has been a challenge, as OT security is still viewed in isolation. This can create significant cyber-exposure and business risk for organizations in the manufacturing, energy, and utility sectors. Recent attacks on industrial control systems (ICS) in Saudi Arabia could have been significantly more destructive. These attacks use Remote Access Trojans that penetrate control systems that operate or automate industrial processes. For example, an attack prevented in 2017 was not only designed to compromise and exfiltrate the data of a petrochemical plant in Saudi Arabia, but was also designed to trigger an explosion. This is a clear indication that cyberattacks present a threat to human life. Cyber-extortion via ransomware is another growing concern. In 2017, Saudi Arabia experienced a crippling attack by the renowned WannaCry ransomware that affected some government entities and Saudi Telecom Company (which was attacked, but without any notable impact on their systems). The attack on Saudi Arabia was one of many that hit dozens of countries around the world in a short time span. Industry experts expect the use of ransomware for cyber extortion to increase rapidly worldwide in the coming few years.²¹

Efforts to Improve Cybersecurity in Saudi Arabia

Despite relentless cyberattacks on the Kingdom, the cybersecurity landscape in Saudi Arabia is improving. The Saudi government has placed special emphasis on cybersecurity with several initiatives, adopting innovative technology policies, and focusing on skills development. In spite of incidents in the recent past, confidence in the Kingdom's security stance is high.

That said, it is extremely important for the Kingdom to protect its critical infrastructure, by taking its cybersecurity maturity and commitment to the next level. The Potomac Institute of Policy Studies in 2017 conducted a detailed assessment of Saudi Arabia's cyber readiness across seven essential elements. This gave Saudi authorities a comprehensive evaluation upon which to base its national cybersecurity policies, including the infrastructure and services upon which its digital future and growth depend.²²

Nurturing National Threat Response Capabilities

Saudi Arabia has placed considerable focus on building its incident response capabilities. In 2016 alone, the Kingdom sustained more than 1,000 cyberattacks on critical national infrastructure with the aim of causing essential service disruption and stealing data.

Although the NISS highlights the importance of threat intelligence sharing and collaboration, a national policy for information sharing is lacking. Saudi Arabia is committed to increasing the levels information sharing around emerging threats, vulnerabilities, and appropriate response and mitigation tactics by developing an information/intelligence sharing policy and a platform to exchange that information. Ongoing efforts to formalize a robust threat intelligence sharing platform that will help the Saudi enterprise community to learn from cyber incidents targeting organizations across Saudi Arabia.

²¹ <https://www.businessinsider.com/ap-the-latest-saudi-arabia-confirms-its-computers-hit-by-virus-2017-5>

²² <https://www.belfercenter.org/publication/cyber-readiness-index-20>

5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment

Threat intelligence services will be delivered by the National Security Operations Center (nSOC), which will collect and disseminate threat intelligence, analyze attacks, recommend mitigation plans, and coordinate a national response. The National Information Security Environment (NISE) team will be responsible for managing and operating the national SOC, together with supporting national-level crisis management efforts and coordinating with relevant stakeholders such as CERT-SA.

Increasing Research and Development Activity Around Cybersecurity

Expanding research and innovation related to cybersecurity through international cooperation is one of the vital aspects of the NISS. In order to increase domestic information security capabilities, Saudi authorities are attending global cybersecurity summits and conferences, investing in or acquiring information security and cybersecurity start-ups, and coordinating and integrating domestic and international research and development efforts. However, certain challenges such as limited government-to-government cooperation and a lack of local cybersecurity experts capable of engaging international cybersecurity communities are impeding the drive for collaborative R&D. To address these concerns, the NISS proposes establishing a research and innovation function that will oversee grants and funding for specific security programs. This is to be part of the King Abdulaziz City for Science and Technology (KACST) and will be coordinated with the Ministry of Communication and Information Technology (MCIT).

Integrating Cybersecurity Competencies into Government and Defense Bodies

Cybersecurity mandates are incorporated into the wider national cyberdefense agenda, which covers several ministries in Saudi Arabia. For example, the Ministry of Defense and Aviation and the Ministry of the Interior are investing heavily in advancing their cybercapabilities. In recent years, Saudi Arabia has also enhanced its collaboration with the United States through a Security Cooperation Agreement. Several mandates aim to improve counterterrorism defense systems, with specific focus on strengthening cyberdefenses and maritime security and equipping Saudi defense forces such as the Saudi National Guard with dedicated cybersecurity and electronic warfare capabilities.

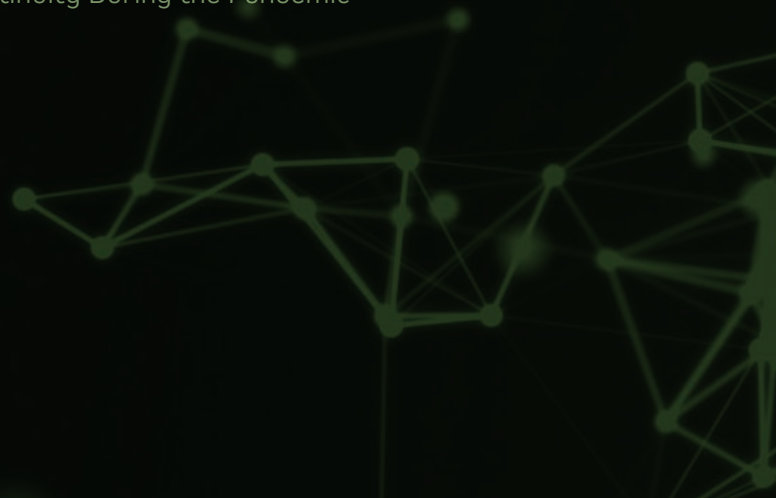


1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment

6

Interview with **Mobily**: Securing the Kingdom's Digital Transformation Journey

7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Interview with Al Moammar Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



ENG. MAJED ABDULAZIZ ALOTAIBI

Chief Business & Wholesale Officer, Mobily



Majed Abdulaziz Alotaibi is the chief business and wholesale officer at Mobily. He joined Mobily in 2016, bringing more than 18 years of executive ICT sales and marketing experience, most of it in the telecommunications industry.

Majed is a highly efficient, innovative, and methodical business leader with extensive experience in B2C and B2B marketing and sales. He leads Mobily's B2B and wholesale business and manages relationships with key accounts at an executive level, including CEOs, SVPs ministers, and vice ministers.

Majed holds a bachelor's degree in Electrical and Communication Engineering from King Saud University, and has completed multiple executive programs with leading international universities like

INSEAD, Hult Ashridge Executive Education, and the University of Chicago's Booth School of Business.

Prior to joining Mobily, Majed fulfilled various different roles for STC over a period of 14 years. In 2009, he introduced multimedia to the Saudi market for the first time by launching IPTV services at STC.

Majed's aim is for Mobily Business to be the trusted ICT provider of choice and an innovative early adopter of new technologies and use cases around cybersecurity, artificial intelligence, big data, and the Internet of Things (IoT) so as to support the development of Saudi Arabia's digital economy and enable the digital transformation of the local B2B market and its customers.

6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey

Q1. How would you describe the importance of cybersecurity in the digital transformation process, particularly given the growing sophistication of cyberthreats?

Digital technologies are transforming the business world, with enterprises increasingly adopting disruptive technologies and swiftly moving their infrastructure to cloud environments.

Modern-day enterprises have been accelerating the pace of their digital transformation, spurred by the adoption of innovative technologies like cloud, edge computing, artificial intelligence, and IoT. However, the more data, applications, and technologies move into the digital realm, the more opportunities arise for hackers and other malicious actors.

Technology has penetrated every aspect of our lives, much more so than just a decade ago. The rapid and widespread expansion of technology has given rise to a variety of malicious cyber elements. Public and private sector organizations are suffering from ever-increasing cyberthreats, hampering the implementation of their digital transformation initiatives. Opportunities and rewards for cybercriminals have increased exponentially due to mass technology uptake, from novice hackers hoping to make a quick buck by releasing ransomware on a single computer to state-sponsored hackers engaging in cyberwarfare. The fact that cybercrime now penetrates virtually every aspect of modern society shows why cybersecurity is critically important.

Most businesses used to think that if they had the latest antiviruses, firewalls, and encryption tools in place, they could leave security to their IT teams and focus on enabling more business. But data breaches and hacks continue to affect companies, causing irreparable damage to their reputations and revenues.

We have already seen the havoc caused by attacks like Ryuk and the Reypson and Lealerlocker ransomware that have affected major organizations all around the world. These attacks have highlighted both the vulnerabilities of IT infrastructures and the

importance of cybersecurity as a vital element of digital transformation.

In a bid to fend off cybercriminals, many enterprises have started to invest in cybersecurity, although the investments are few and far between, mainly due to the cost of implementation and the complexity of solutions available on the market.

Q2. With the public sector leading the Kingdom's digital transformation efforts, what is your view on the various initiatives that the Saudi government has launched to improve the local cybersecurity landscape?

Saudi Arabia is at the forefront of cybersecurity in the region. To protect the Kingdom's critical ICT infrastructure, King Salman issued a royal decree in 2017 to set up the National Cybersecurity Authority (NCA). The primary role of the NCA is to provide policies, frameworks, standards, and guidelines in order to protect Saudi Arabia's critical ICT infrastructure and, in turn, improve the cybersecurity posture of the Kingdom.

The Saudi government is making great strides in terms of adopting agile and dynamic strategies to identify and respond to the evolving security threats. In addition to providing standards, frameworks, and guidelines, the NCA is organizing awareness events and hackathons, with the aim of driving international cooperation in the cybersecurity domain and creating an environment where well-formulated ideas and initiatives are exchanged between the international cybersecurity community.

It is important to note that even before the establishment of a dedicated cybersecurity authority, Saudi Arabia has consistently shown a high regard for cybersecurity, actively protecting its national institutions from malicious attacks through the deployment of innovative security solutions.

Another major focus of the NCA is to attract national and international organizations to build

6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey

partnerships with public and private entities to stimulate innovation and investment in the cybersecurity domain. This will help Saudi Arabia achieve a technological evolution that is specifically aimed at serving the future of the Kingdom's diversifying economy.

Anticipating and reacting to cyberattacks has become a necessity, especially for government agencies that are dealing with critical information and citizen data. Under the leadership of King Salman and Crown Prince Muhammad bin Salman, Saudi Arabia has made it clear through the establishment of the NCA and several cybersecurity initiatives under Vision 2030 that the Kingdom prioritizes information security, business continuity, and the protection of sensitive data with swift responses to cyberattacks.

Q3. What are the key activities your organization has undertaken to enable the government's vision to strengthen Saudi Arabia's cybersecurity outlook?

Cybersecurity is at the core of Mobily's ICT service offerings, as well as its own internal operations. In line with the Kingdom's Vision 2030 and National Digitization initiatives and strategies, Mobily provides a comprehensive ICT portfolio to both the public and private sectors, across industries. Our information security services contribute significantly to ensuring proactive prevention and fending off cyberattacks around the clock.

To showcase our commitment to Vision 2030, National Digitization, and the evolving business landscape of the Kingdom, Mobily has created a vast portfolio of security services that are hosted locally in a state-of-the-art security operations center at our Uptime Institute-certified Tier 4 Operations Gold Certification datacenter. Mobily takes pride in offering these services as part of our strategic longstanding partnerships with leading global service providers. Our cybersecurity solutions use data analytics to help enterprises understand their security posture and protect their critical ICT infrastructure.

With decades of industry experience and a robust global partnership network, we can analyze attack trends and threats, enabling enterprises to make well-informed, data-driven decisions. These security solutions are provided as per global standards through Mobily's partnership with a wide array of well-established partners. For example, research indicates that DDoS is the number-one threat to the availability of services, where the fundamental goal of an attacker is to create maximum disruption at peak operation times.

To counter this, Mobily has created a dedicated cloud-based DDoS Service that proactively monitors a client's traffic patterns from core or edge devices to detect attacks in real time. Similarly, Mobily's cloud security portfolio includes a wide range of services ranging from penetration testing, phishing protection, and ransomware detection and avoidance — all of which ensure that enterprises in the Kingdom are meeting the government's regulatory criteria by protecting themselves from cyberattacks.

Q4. IDC research shows that managing enterprise security is the biggest technology-related challenge facing CIOs today. What challenges do you see arising as innovative technologies (like IoT, cloud, artificial intelligence, etc.) drive digital transformation initiatives?

The cybersecurity war continues to be ever evolving. Attackers are persistent, unleashing attacks with increasing frequency and complexity. They have access to toolkits on the dark web and from several marketplaces that enable them to customize their attacks. The shortage of skills to counter these attacks and mitigate the potential threat exacerbates the issue.

Malware is one of the costliest and most common cybersecurity threats in the digital world, with unprepared organizations often having to pay cybercriminals hundreds of thousands of dollars— if not millions—to halt data breaches and virus attacks.

6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey

The proliferation of IoT is another area for concern. All these connected devices make our lives easier and more comfortable. For example, our electricity meters can communicate directly with our energy provider in real time to enable faster and more accurate billing. But as more and more devices become connected and generate and share data, that data and the networks it resides in are highly prone to cyberattacks. Insecure web interfaces, insufficient authentication protocols, and a general lack of cybersecurity knowledge create numerous vulnerability points for malicious attacks on endpoints, gateways, edge devices, and even wearables.

Serverless applications will represent another big threat in the years to come. The technology entices cyberattacks, since the data is stored on a device instead of in a secure cloud. Getting access to users' devices through malware or physical theft is far easier than breaking through encryption, firewalls, or a secure cloud typical in traditional server-client setups. With serverless applications, the safeguarding of data is predominantly the responsibility of the user.

But it is not all doom and gloom. The expansion of artificial intelligence and blockchain promises improvements in the cybersecurity posture of the enterprise ecosystem. Bots with AI-assisted threat detection capabilities will soon be available. There's no doubt that, in the future, it will be common for humans and AI to cooperate to defend critical data and digital infrastructure. The same goes for blockchain — several global ICT providers are working on developing a wide a range of use cases, medical records, real-estate deeds, and identification data to improve security. As these use cases mature, public and private blockchains will be integrated with traditional cybersecurity practices.

Q5. How prepared is the Kingdom when it comes to securing these technologies?

The Kingdom is well prepared, and preventive measures are being undertaken. Enterprises across the Kingdom are now required to have minimum measures in place to defend against cyberthreats. However, the proliferation of IoT and other emerging technologies that expand the attack surface is making this a difficult task, putting core systems and data at risk. IoT devices can be hard to patch since some of them do not have a physical UI or screen for users to apply an update. As such, the Kingdom's relevant authorities are establishing policies and procedures based on which actions (data collection, software updates, etc.) can be performed on IoT devices.

A prime example is the Ministry of Interior's specifications for enterprises deploying CCTV security and surveillance systems. The Ministry outlines the features that a CCTV camera should have for each industry, as well as the type of encryption, storage, firewalls, and connectivity required as a bare minimum.

Similarly, Saudi Arabia has introduced its own Cloud First Policy that highlights public sector migration from traditional IT solutions to cloud-based models in a secure manner. The policy recognizes cloud computing advantages such as enhanced agility, reliability, security, and innovation.

Such initiatives demonstrate that Saudi Arabia is taking cyberthreats seriously and is willing to adopt a preventive and proactive approach, not just by deploying innovative solutions, but also by laying robust regulations for public and private sector entities.



1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey

7

Cybersecurity Challenges in Today's Digital World

8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation
10. Interview with Al Moammār Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



CYBERSECURITY CHALLENGES IN TODAY'S DIGITAL WORLD

Technological advancements in the internet era have transformed societies in ways that science fiction writers 100, 50, or even 25 years ago could never have imagined. How we communicate, learn, and go about some of the basic facets of day-to-day life have radically changed. The disruptive nature of technological progress has radically transformed every aspect of society, permanently changing how aspects of our lives are governed, as well as how businesses and government bodies perform their functions.

Look at the ways that information is transmitted. Maps on our smartphones have effectively removed the need for printed maps. People just say, "Okay, Google" or "Hey, Siri" to get their smartphone to give directions from wherever they are to anywhere they wish to go. Road information is processed by Internet of Things (IoT)-enabled video cameras to enable real-time road conditions to be processed and passed along to IoT-enabled car stereo screens.

As amazing as those advancements are, consider some of the other completely new industries that have sprung up due to the immediate availability of massive amounts of data. Uber and Lyft have decimated the taxicab business, as everyday people are now able to earn extra money shuttling people anywhere they wish to go by just launching an app on their smartphone.

Hungry? That same company, Uber, that can provide a driver to take anyone anywhere can now receive orders for breakfast, lunch, and dinner from a myriad of restaurants. These orders can seamlessly be fed into the point-of-sale (POS) systems at these restaurants with the order, customer information, and — in some cases — the payment information attached to that order.

That hungry consumer, who gets that dinner delivered to his home, can sit down and enjoy a movie that is suggested to him by the Amazon Prime Video service he subscribes to, based on his prior movie watching history. After a nice movie dinner, he can skip driving to the local shopping mall to buy a birthday present for his younger brother and, instead, use the same company that provided him with his movie, Amazon, to ship that new set of golf clubs to his brother.

Technological Changes Go Beyond the Consumer

The technological innovations that have transformed the lives of everyday consumers have also drastically increased the vulnerabilities that businesses and governments must address in order to protect the vital data with which they have been entrusted. Increasingly, the private data that must be protected, reported on, and updated is in one, two, or many different clouds. Keeping track of all the data being stored in disparate clouds is difficult. What becomes almost impossible is the absolute need not only to make this data available in a moment's notice, but also to keep it secure from the cyberwarfare that is increasingly being launched by rogue nations and other cybermiscreants.

As businesses and governments struggle with the digital transformations (DX), which have caused the explosion of data in datacenters, cloud environments, and edge locations, security practitioners are increasingly playing catchup to try to secure their infrastructures. Too often, they are thrust into situations where security is bolted on at the end of a project, rather than having security being part of the DNA at the project's onset. Security is too often an afterthought, rather than being front of mind to the DevSecOps teams developing the applications in this new cloud-focused world.

Increasingly, even objects within the home, such as home routers, thermostats, and refrigerators, can become weaponized to launch denial of service attacks against targets, including critical infrastructure such as utilities and transportation systems. All too often, these IoT systems are equipped with very basic security, lack disciplined patch management, and utilize default passwords that are seldom changed. Consequently, IoT devices and systems are vulnerable to cybercriminals and nation states to install malware on these devices, making them unwilling participants in cyberwarfare campaigns.

To make matters even more challenging, cyberwarfare is becoming a common tactic not only to impact individual businesses, but also to go after a country's vulnerable industries. Vulnerable assets such as electricity grids, nuclear power plants, and oil refineries no longer need to be physically attacked by bombs or missiles to be taken out. Instead, highly targeted attacks can be put together to plant malware within the IT structures that operate these assets. The loss of trust in key institutions unable to protect themselves against these cyberattacks can disrupt economies, resulting in economic and political turmoil, all without a single bullet or missile being fired.

This new arms race, just like the buildup of missile defenses that are commonly being deployed to protect military bases and population centers today, is also occurring within federal and local governments, military institutions, and the security operations centers (SOC) that protect businesses. Governments and businesses need to have within their means the capabilities to protect the assets with which they have been entrusted.

Just like armies need soldiers and navies need sailors, countries need to recognize that it is now a matter of national security that they can properly staff the SOCs with the security operations analysts that operate on the frontlines of this new cyberfront. Properly trained cybersecurity professionals take time — months or years rather than days or weeks — to become fully proficient in their craft. Trade schools, colleges, and universities need to become active partners with the businesses, governments, and military institutions to provide these new “cyber-foot soldiers” in this new era.

Traditionally, these future cybersecurity professionals have been culled from the science, technology, engineering, and math (STEM) programs that traditionally feed computer science programs in colleges and universities, but these talented people are difficult to find and costly to hire. In the cyberwarfare arena, not all security operations personnel necessarily need to come from the STEM environment. Some of the

7. Cybersecurity Challenges in Today's Digital World

activities that are vital to protecting and responding to cyberthreats take people with other skills, such as strategy, creativity, and psychology, which are more often found within the walls of the liberal arts or other collegiate programs of higher learning.

Challenges in Cybersecurity

How do organizations go about getting help to secure their applications and data from all threats, which seem to grow exponentially? It starts with two accepted principles.

The first principle is that no one person, process, or technology will lock down the growing risk surface that DX projects create. The mythical magic bullet to protect organizations does not exist, but that does not mean that no path forward exists to protecting these critical assets if proper leadership is put in place. Cybersecurity textbooks, and even certain regulations, will mention that a proper first step is to put in place a senior manager to oversee cybersecurity. A common title for this person is chief information security officer (CISO). Having the right leadership of the cybersecurity department is the starting point from which all other cybersecurity initiatives will flow.

The second principle is that security cannot be the exclusive domain of the CISO and the members of the cybersecurity operations team. As with IT initiatives, which no longer consist of simply having new applications and services put into production without working with lines of business, recognition and appropriate organization-wide priority need to be given to the CISO's team for it to be successful. This team must work with colleagues at all levels of the organization, from the boardroom to the operator.

CISOs can deploy the best firewalls, world-class threat intelligence platforms, and 24x7 coverage in their SOCs, but all of this can be taken down when an HR manager with the same password in social media as the company's human relations management system (HRMS) has his password stolen and the payroll history of the company's top employees is leaked. It only takes one missed step for an organization to face massive losses in brand integrity, as well as financial losses from the regulatory fines and outside assistance needed to respond to the breach.

Keeping in mind these two principles, CISOs need to address several challenges to perform their important roles.

CISOs Need Assistance

As CISOs work to improve the effectiveness of their teams, they often come to recognize that, besides corralling the assistance and cooperation of their coworkers and the C-Suite, they sometimes need to reach out to other firms to aid them in fulfilling their mission statements of protecting their organizations from cyberattacks. This aid often comes in the form of services provided by managed security service providers (MSSPs).

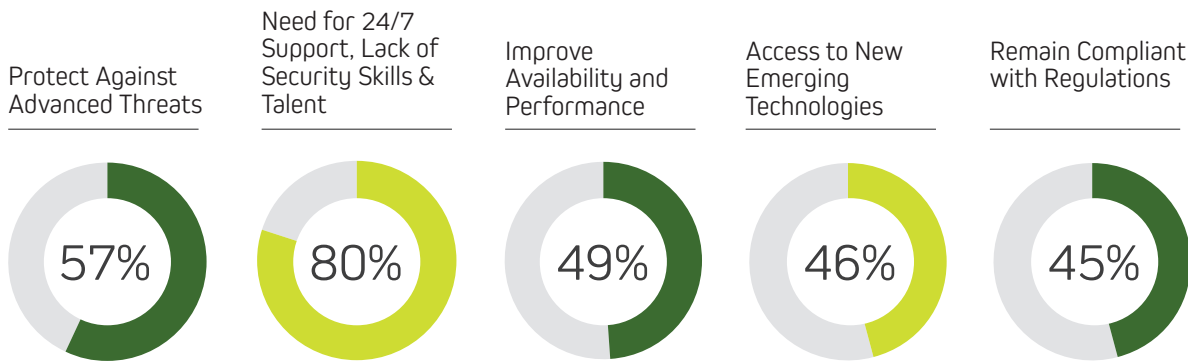
It should not come as a surprise to see the recent growth of MSSPs and the related growth of other professional security service components, such as IT consulting and systems integration, which support these vital security services. IDC projects that the combined managed and professional security services global market will expand from \$47.5 billion in 2018 to \$80.1 billion in 2023.

The security services market is growing for a variety of reasons. **Figure 5** shows responses in a recent IDC survey of CISOs and others responsible for cybersecurity. One of the top reasons for respondents partnering with an MSSP to provide security for their firms was that adversaries are getting smarter and

7. Cybersecurity Challenges in Today's Digital World

creating attacks that are more complex and harder to detect. Organizations recognize the need to see what is occurring across the security landscape, especially as the attack surface grows with the rush to cloud computing.

FIGURE 5 – Top Reasons for Using a Managed Security Service Provider



Source: IDC's Managed Security Services Survey, January 2019

The targeted nature of attacks is growing more advanced every year. Cybercriminals, and/or the nations that launch cyberattacks or support these cybermiscreants, are able to tailor these attacks based on publicly available information found on social media or by purchasing personally identifiable information (PII) at relatively low cost on the dark web. Malware exploitation kits, with malware specifically tailored to infiltrate an organization's defenses, are increasingly being used to launch their payloads. In addition to these capabilities available for purchase on the dark web, hackers can purchase distributed denial of service (DDoS) kits, which can shut down an organization's network, website, or network services.

CISOs constantly find that the people leg of the cybersecurity tripod (people, processes, and technology) is often the hardest to manage. Simply securing the day shift of the organization's SOC is no longer enough. Organizations must also worry about threats that come in during non-business hours, as the survey results show.

Today, more than ever, the need for 24x7x365 support is crucial. As part of this coverage, a follow-the-sun approach is needed to provide the best possible coverage in the SOC. The SOC day shift is usually filled with the best talent. In a follow-the-sun approach, SOCs are located around the world for 24-hour coverage, enabling the provision talented staff around the clock.

The understanding that cybercriminals require just one opportunity to expose a company's resources is also driving recognition that the availability and performance of the platforms and services protecting firms today need to be elevated. This includes getting all systems properly installed, configured, tuned, and continuously available. MSSPs have often become a resource that is leveraged to get platforms and services properly configured. Their expertise lies in applying the technical solutions necessary to ensure disparate systems talk to one another and connect to central data repositories and sources, such as data lakes and security-information-and-event-management (SIEM) tools, to correlate data to detect potential attacks and breaches.

7. Cybersecurity Challenges in Today's Digital World

Another high priority area in which organizations look for help from MSSPs is maintaining compliance with ever-increasing regulations from governments and regulatory bodies all over the world. CISOs struggle, especially in smaller organizations that do not have access to full-time legal counsel to keep track of all the different regulatory requirements. Many of these regulations are confusing, and organizations might be tempted to erroneously think they do not fall under the regulatory mandates. Almost as bad, they might attempt to maintain compliance but then find their systems are incapable of providing the proper reporting to comply.

Too Many Vendors and Point Products to Manage

As previously mentioned, CISOs are charged with protecting their assets in the cloud, at the edge, and in corporate datacenters. Often, over the course of time, organizations acquire point products from many different providers. Sometimes, they even have overlapping products to fill essentially the same role, such as different endpoint security products and different firewalls. Having different products that fill the same or very similar roles from different providers is both a productivity and a financial drain.

All these products require configurations, maintenance, training, and upgrades to fulfill a specific function. CISOs and other security professionals find themselves spending time managing the different licensing requirements and having to keep security providers abreast of changing network configurations to get the proper technical assistance.

CISOs are cognizant of the time wasted on too many vendor phone numbers in their contact list and too many point products to maintain in the SOC. Reducing not only the number of point products, but also the number of vendors utilized is slowly becoming the new mandate in the SOC. This situation has contributed to the rising adoption of security platforms, as discussed later in this report.

Defending the Constantly Changing Network Perimeter

Another challenge CISOs face is foundational changes to the network topology, which have to be defended. Earlier, network infrastructure was simpler. Datacenters were the primary asset and housed all the crown jewels, such as web servers, databases, and file servers. Other sites also had to be secured, such as branch offices, but they were kept safe by backhauling their internet traffic through expensive and difficult-to-maintain MPLS connections.

As cloud evolved, IT departments and security-operations teams found themselves playing catch up to newly consumed services from the cloud — such as Salesforce, Slack, and Yammer — provided by shadow IT. Shadow IT relates to employees outside of IT using and creating services, primarily based in the cloud, without IT oversight or authorization. This is often a direct outcome of the IT department — or, more recently, the cybersecurity team — not being able to meet the application needs of their internal customers in a timely or suitable manner.

Having a collaborative environment within an organization, eliminating walls or boundaries between the cybersecurity team and other departments, can help to ensure safe DX transitions. The most effective cybersecurity teams engage throughout the process of migrating data and applications from corporate datacenters to the cloud and edge, where so much development is occurring today.

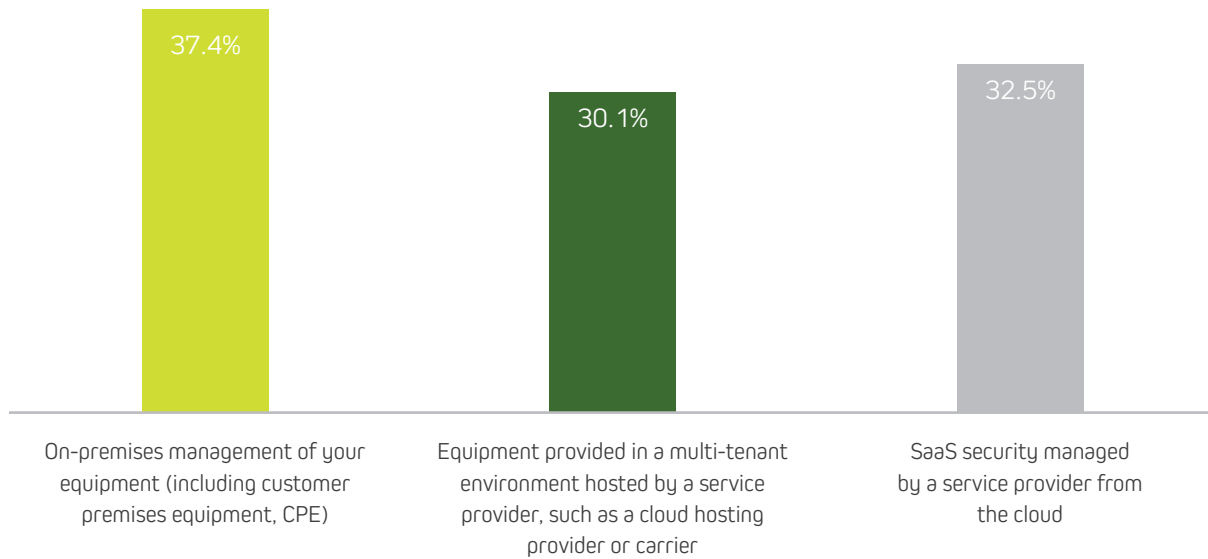
Given the greater availability of mobile data using 4G and 5G implementations, along with burgeoning computing capability at the edge, the perimeter has become harder to defend, as it has been stretched to breaking point at times.

7. Cybersecurity Challenges in Today's Digital World

MSSPs have been sideline witnesses to this change, as they see a soaring need for their services to secure organizations' far-flung assets. **Figure 6** shows how more than 60% of managed security services are now focused on the management of equipment in either third-party or software-as-a-service (SaaS) environments.

FIGURE 6 – Breakdown of Spending on Managed Security Services in the Past 12 Months

Q. How does your spending on managed security services purchased in the last 12 months breakdown based on the following?



Source: IDC's Managed Security Services Survey, January 2019

All these changes in the basic structure of the network, largely as a result of DX efforts, have resulted in additional friction between stretched cybersecurity teams and their counterparts in IT and elsewhere in the organization. These moves away from a more formal or traditional network structure have come at the expense of taking a holistic view of how to secure these new endpoints.

The phrase “bolted on security” is one that sends shudders through CISOs, as this is a recognition that security was not a part of the design of these new networks. Instead, more often than not, the security aspects are put in place after the applications and data have already been exposed outside of the corporate network environment.

If organizations ever hope to reduce the attack surface exposed to potential cyberattacks, their various departments will need to learn to collaborate with the security operations teams to have security best practices as a part of the DNA of these DX projects.

Scarcity of Qualified Information Security Professionals

One of the hardest challenges that organizations face in improving their security posture is a lack of qualified personnel to install, maintain, and manage all the required products and services. The cybersecurity profession seems like it is perpetually catching up to provide the security practitioners necessary to fill these crucial roles.

7. Cybersecurity Challenges in Today's Digital World

The International Information System Security Certification Consortium, or (ISC)², conducted a study in 2019 to consider the current number of people employed in the cybersecurity profession and the number of openings for various jobs in this field. As per their analysis, the gap between the number of people working in the cybersecurity domain and the number needed is staggering. The United States alone has a shortage of nearly half a million people. Globally, the estimated shortfall is over four million people.

Any good economist can explain what this shortfall can produce. The lack of qualified security practitioners to fill these crucial jobs has resulted in higher prices for the salaries of those people who are filling the positions. For organizations that are unable to find qualified people, they often turn to MSSPs to perform those functions, or they utilize a services model whereby they have specific functions that they need filling in their cybersecurity teams performed by an MSSP.

For example, instead of trying to find personnel to perform threat intelligence functions, like deep- or dark-web searches for potential adversaries, organizations can far more quickly turn to an MSSP to fulfill this vital function. The practices required to perform the necessary intelligence gathering to find threats to an organization and its associates are very time consuming, and the skills involved take a long time to acquire. As a result, organizations are often turning to third-party companies to perform such functions on their behalf.

Continued Growth of Compliance Regulations

Governments are increasingly concerned about the damage that can occur when cyberattacks are launched, damage that stretches to the privacy and finances of their citizens. In an effort to protect citizens from the effects of cyberattacks, governments and regulatory bodies are increasingly passing laws and regulations to force organizations to take the appropriate steps to protect themselves and the private data they have in their custody.

Publishing an exhaustive list goes beyond the scope of this document, but below is a relatively broad sampling of some of these laws and regulations:

- The European Union's General Data Protection Regulation (GDPR), which went into effect in May 2018, is a broad and far-reaching regulation that gives the residents of EU member states broad rights on how and where their personal data is processed. Here are a few examples of the many rights that the EU bestows on citizens within the Union through GDPR:
 - » Any company holding the personal data of EU citizens, regardless of the location/country from which the company operates, must offer each EU citizen the right to retract the data he or she initially shared just as easily as it was for him or her to provide that information in the first place.
 - » Organizations that handle EU citizens' personal data are mandated to apply appropriate measures to protect that personal data. Any data breach that touches upon EU citizens' personal data must be reported within 72 hours.
 - » Violations of GDPR regulations can result in fines of up to €20 million, or up to 4% of the firm's prior year revenue, whichever is higher.
- In the United States, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 has a portion of the law devoted to protecting patient data. This law, in conjunction with the guidelines set out in the Health Information Technology for Economic and Clinical Health (HITECH) Act and other regulatory expansions, have raised the bar in terms of requirements and potential fines for failure to follow the regulations to safeguard Protected Health Information (PHI).

7. Cybersecurity Challenges in Today's Digital World

- » Some of the requirements include the need for businesses to ensure the confidentiality, integrity, and availability of all PHI they create, receive, maintain, or transmit. In addition, they are to protect against reasonably anticipated threats to the security or integrity of the PHI that they manage.
 - » In the event of a breach, affected individuals are to be notified within 60 days. If the breach affects more than 500 individuals, then the entity must report the breach to the media and the Office of Civil Rights (OCR), where the information is publicly posted online on a forum labeled the Wall of Shame.
 - » Failure to follow the regulations during an incident or as a result of findings from an audit can result in fines of up to \$1.5 million.
- Regulations can even extend down below the national level, as witnessed in the United States with the New York Department of Financial Services (NYDFS) Cybersecurity Regulation. This regulation affects insurance companies, banks, and other regulated financial services organizations and features a laundry list of requirements with specific timelines that must be met once an entity is deemed to fall within its regulatory oversight. This wide-ranging regulation has many requirements to which firms must adhere, such as:
 - » Financial services companies must have a chief information security officer (CISO) or a third-party service provider (e.g., an MSSP) to act as a CISO.
 - » Financial services must conduct an annual penetration test and continuously monitor the effectiveness of the cybersecurity program and must fulfil an annual risk assessment.

The various privacy and cybersecurity laws and regulations with which companies must comply may initially appear as just additions to a growing list of mandates for organizations. Taking a longer view of overall improvements to the organization's cybersecurity posture makes it easier to accept that most, if not all, of these regulations are beneficial. With the increased hardening of the cyberinfrastructure resulting from new cybersecurity regulations, organizations can look forward to increased levels of trust being applied from all relevant stakeholders, as well as the reduced likelihood of a cyberattack applying a fatal blow.

The Issue of Trust

A final challenge that CISOs and the C-suite need to recognize involves the issue of trust. Organizations today are no longer islands unto themselves. They increasingly have vendor relationships in which the risk to their intellectual property is exposed in order to streamline supply chains, provide better services to customers, or reduce costs by outsourcing commoditized back-office functions. In the event of a breach caused by a third-party vendor, the consequential news reports are more likely to highlight the larger company's profile, impacting their ability to position their business in a positive light.

But how do organizations determine for which relationship is it worth accepting some level of risk, and how is that risk level measured? Reviewing the cybersecurity policies and procedures of the third party is obviously a prudent first step, but these efforts require a significant investment in human hours. As soon as their programs have been evaluated and the risk and vulnerability assessments have been performed, these initially valuable insights become dated the next time a new API becomes available or a new edge location is established.

Company boards of directors (the C-suite) increasingly consider the risk scores of the firms with which they engage, but obtaining such profiles is challenging — especially given that CISOs hesitate to divulge information about their cybersecurity approaches for fear that such information could be used against them in the form of targeted malware.

Steps to Advance Cybersecurity Practices

CISOs can take various steps to advance cybersecurity practices within the organization. Some firms will attempt such steps on their own, while other firms will increasingly engage an MSSP to provide a part of or all the functions necessary to achieve a strong cybersecurity posture. / The below-outlined steps provide a foundation upon which other capabilities can be launched. These steps, however, should not be considered an end but a beginning in the CISO's journey to securing the organizations assets.

1. Follow an Established Framework

New or revamped cybersecurity programs should follow a recognized framework. Various frameworks can be followed, such as the ISO/IEC27000 standard, Payment Card Industry (MasterCard data security standard), or Center for Internet Security (CIS Benchmark). The U.S.'s Cybersecurity Framework of the National Institute of Standards and Technology (NIST) is among the more commonly followed and recognized frameworks — one that can also be used to provide concrete steps and guidance on measuring the effectiveness of an organization's cybersecurity program.

The five core functions outlined in the NIST framework are:



Identify



Protect



Detect



Respond



Recover

Organizations must recognize that breaches will occur and put mechanisms in place to detect, respond, and recover when they happen.

2. Utilize Firewalls and/or UTM/IDS Devices

The days of IT personnel reviewing Active Directory event logs or router and firewall logs to ascertain possible signs of a breach are long gone. The implementation of a unified threat management (UTM) system is usually the first security precaution taken, since UTMs generally encompass not only a firewall, but also an intrusion detection system (IDS) to examine network traffic for signs of malicious intent.

Among the other capabilities often included within a UTM device are email filtering (often with third-party spam filter lists), virtual private network (VPN) capabilities, antivirus (AV), and web-content filtering.

3. SIEM

Implementing a UTM with a firewall is a great first security step, but it is by no means enough on its own. An SIEM solution is another cornerstone of good cybersecurity hygiene — one that has many components. For example, not only do SIEM systems aggregate data from multiple sources (IDS systems, firewalls, routers, servers, etc.) to show patterns that might indicate potential breaches or other cybersecurity issues, but they also feature dashboards to provide a holistic overview of cybersecurity posture.

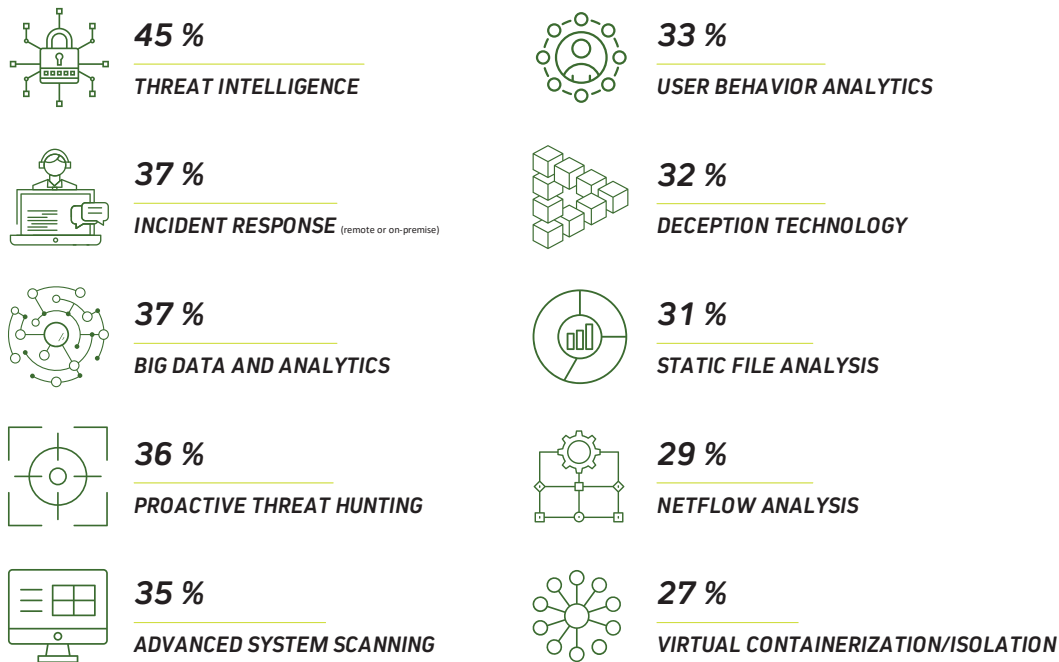
7. Cybersecurity Challenges in Today's Digital World

4. Leverage Threat Intelligence

Monitoring threat intelligence feeds that are relevant to and focused on the organization's specific attack surfaces marks another step toward cybersecurity maturity. **Figure 7** shows that many firms will be looking to implement threat intelligence as a key advanced detection and analytics method over the next couple of years.

FIGURE 7 – Advanced Detection and Analytics Techniques/Methods to Implement in the Next 1–3 Years

Q. Which advanced detection and analytics techniques/methods do you think should be implemented in the next 1–3 years?



Source: IDC's Managed Security Services Survey, January 2019

Cybercriminals and/or nation-state sponsored attackers are utilizing targeted attacks that utilize information available at reasonable prices on the dark web. These personalized attacks can often be prevented if a seasoned security analyst is utilized to ascertain whether any potentially harmful information is available on the dark web.

5. Embrace the Zero Trust Journey

As previously mentioned, the traditional network perimeter has undergone some major changes over the years. In moving to a more proactive cybersecurity posture, CISOs are starting to recognize that they must be able to defend the actual assets they are entrusted to keep secure and cannot assume that the network perimeter has not been breached.

To move to this higher level of cybersecurity, they are adopting zero-trust model. The principle behind this is that the systems, data, and devices worthy of protection cannot rely on an all-encompassing firewall to protect everything behind it. Instead, it starts from the premise that you cannot trust anything within the network, or outside it, without the other device/application/user providing credentials to authenticate itself. Instead of trusting anything within the local network, it comes up with the principle that you treat

7. Cybersecurity Challenges in Today's Digital World

the asset that needs to be defended as if it were located external to the local network. In a perfectly laid out zero-trust model, accessing the organization's assets would be the same whether from a Starbucks or from the company's datacenter.

6. Use Managed Detection and Response (MDR)

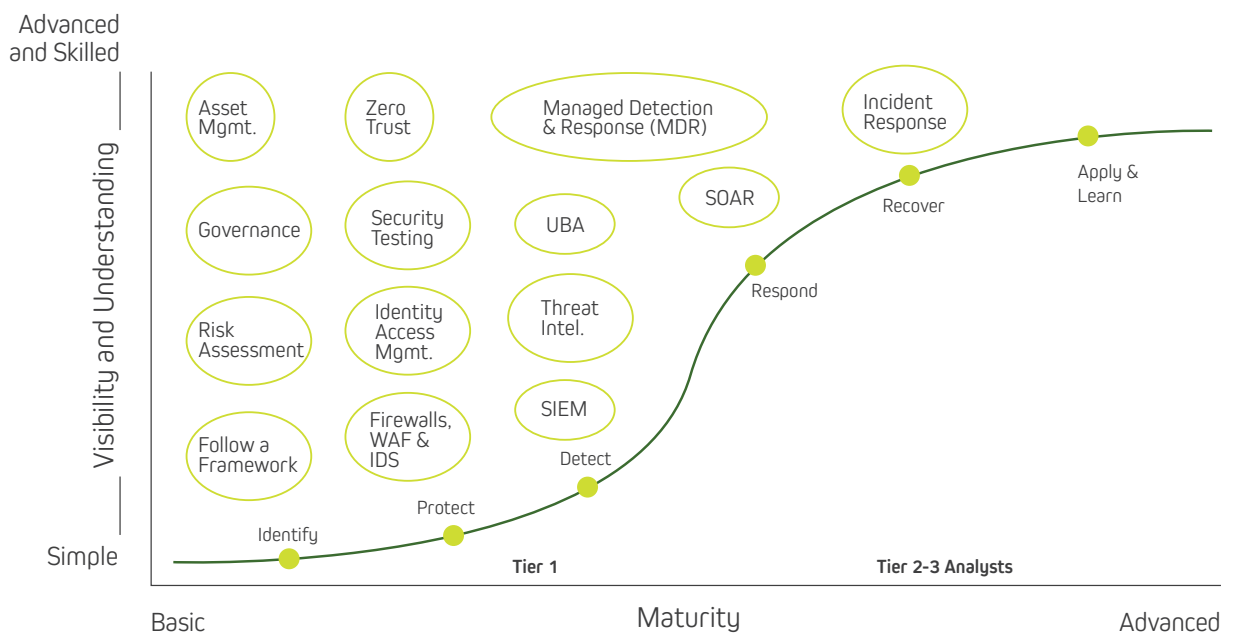
A key initiative being employed to move cybersecurity programs from a reactive to a proactive model is the deployment of managed detection and response (MDR) services. This is not the only platform or service a firm will utilize as it increases its cybersecurity maturity, but it is certainly one of the most comprehensive services that can be put in place. MDR represents a combination of key cybersecurity-program components:

- Threat detection (EDR/XDR)
- Threat hunting
- Incident analysis (forensics)
- Remote incident response services (containment, removal, remediation)
- Threat intelligence
- Human expertise

While some or all of these capabilities may already exist, it is the bundling of these capabilities utilizing advanced technologies such as Big Data analytics and machine learning, along with a strong incident response retainer to handle larger breaches, that truly moves a firm to a highly proactive cybersecurity posture.

The above steps and the core functions shown in **Figure 8** are central to strengthening of an organization's cyberinfrastructure.

FIGURE 8 – Steps Toward Cybersecurity Maturity



Source: IDC, 2019

7. Own Internet-of-Things (IoT) Security

The numbers and diversity of unsupervised sensor-equipped/Internet-of-Things devices in organizations' networks are increasing. Whether in manufacturing, healthcare, retail, or building management (e.g., climate control), connected devices across all industries is on the rise. So, too, is the need to mitigate the risks these devices present without interfering with each device's legitimate function or business purpose.

While approaches will vary, the objectives in exerting security controls are uniform. Those control objectives are:

- **Confidentiality:** Protect sensor-based data from being disclosed to unauthorized entities or individuals.
- **Integrity:** Validate sensor-based data and protect it from being manipulated or identifying changes as it is accessed and/or transmitted over time.
- **Availability:** Allow the intended use of sensor-based data for productivity and other purposes.

In accomplishing these objectives, several security functions will be needed to control information flow, isolate applications, monitor for instances of software modification and/or hardware tampering, and remediate for known vulnerabilities. The challenge IT and security teams will encounter and must address is responsibility. For instance, is the device manufacturer, the device installer, or the organization's IT and security staff responsible for IoT security? The answer, unfortunately, is neither uniform nor static over time. Nevertheless, organizations that rely on IoT devices for their businesses ultimately must be responsible even though they may lack full control (e.g., over firmware integrity). Consequently, they must coordinate across all the involved parties to ensure IoT security is faithfully and comprehensively accomplished.

Next Steps

All the systems and services outlined here are of benefit to any CISO in the performance of due diligence to protect the assets. A cautionary note is relevant here: These steps should never be considered complete because the cybercriminal who wishes to cause havoc at his targets does not recognize any rules in his mission. His capability to evolve and beat any security defenses an organization puts in place should not be underestimated.

In order to thwart the cybercriminal and the nation-states that often fund their exploits, the CISO needs to continually work to improve the cybersecurity tripod (people, processes, and technologies) used to defend the organization. If any one of leg fails to improve over time, the cybercriminal will find this weakness and exploit it. Strengthening the tripod by making the right investments and improvements in each leg will pay dividends over time.

Digital transformation (DX) has been mentioned briefly in this chapter. In the next chapter, we delve deeper into DX, its implications for cybersecurity and trust practices, and how IDC envisions organizations and cybersecurity vendors adapting to the added challenges that DX presents.

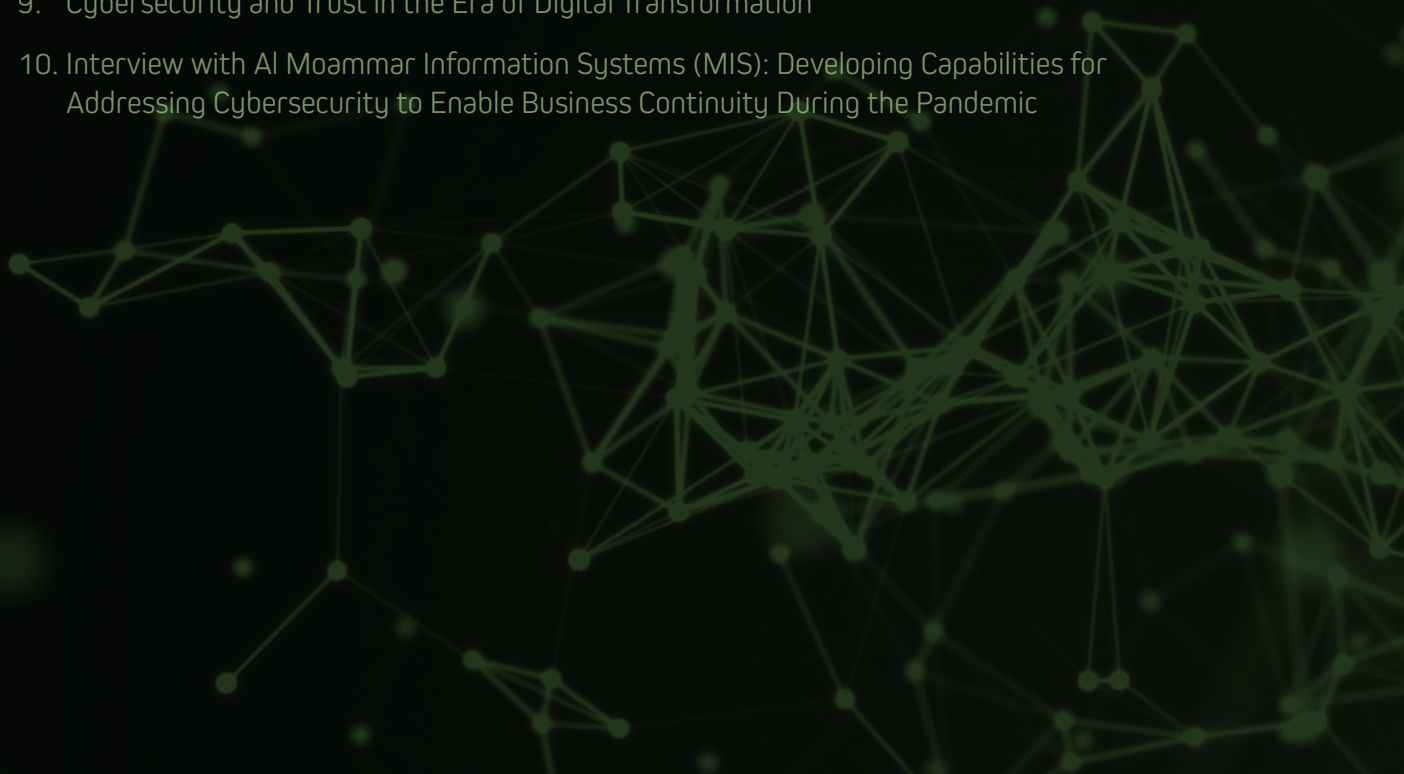


1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World

8

Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World

9. Cybersecurity and Trust in the Era of Digital Transformation
10. Interview with Al Moammar Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



SALMAN ABDULGHANI FAQEEH

Managing Director, Cisco Saudi Arabia



Salman A. Faqeeh is the managing director of Cisco Saudi Arabia. In this role, he is responsible for the execution of a country-wide vision and strategy that delivers value to Cisco's customers and partners. He also works closely with public and private sector organizations to support them on their digital transformation journeys.

Faqeeh is responsible for leading Cisco's business and operations in the Kingdom and for driving the digitization agenda across all industries, in line with Vision 2030 and the National Transformation Plan.

Faqeeh has over 16 years of experience in the IT industry. He joined Cisco in August 2006 and has worked in several roles since, leading key accounts and building strong relationships across sectors, including defense, healthcare, and energy. He also

managed and led the Services business for more than five years, starting in 2012. Most recently, Faqeeh was operations director for Cisco Saudi Arabia, where he led and managed the Public Sector business in the Kingdom.

Prior to joining Cisco, Faqeeh worked with Microsoft Arabia, where he managed relationships with telecom operators in Saudi Arabia, the Ministry of Communications and Information Technology (MCIT), and the Communication and Information Technology Commission (CITC).

Faqeeh holds a bachelor's degree in Management Information Systems (MIS) from King Fahd University of Petroleum and Minerals (KFUPM) in Saudi Arabia.

Q1. How would you describe, in a few sentences, the importance of cybersecurity in the context of the ongoing digital transformation, especially with the growing sophistication of cyberthreats?

As people around the world become increasingly interconnected, and our collective dependence on technology grows, so too does the prevalence of cybersecurity threats. This is especially evident in our region, and Saudi Arabia is not an exception — the strong economy and geopolitical position make the Kingdom a prime target for cybercriminals. That's why malicious hackers continue to devote their time and energy to finding ways around even the most advanced security measures. As a result, data breaches in the Kingdom are now more costly than anywhere else in the world, other than in the United States. With companies in Saudi Arabia particularly keen on embracing digital transformation, industry professionals are fast realizing the necessity for robust cybersecurity measures to aid a smooth journey.

Q2. With the public sector at the helm of digital transformation in the Kingdom, what is your view on the various initiatives that the Saudi government has launched in order to improve the local cybersecurity landscape?

There is no question that Saudi Arabia is leading the Gulf in terms of cybersecurity. Most recently, the Kingdom was ranked first in the region for cybersecurity capacity-building and cooperation by the Global Cybersecurity Index. This ranking is well deserved, especially considering the Kingdom's many recent and ongoing initiatives — notably those supported by the King Abdulaziz City for Science and Technology, which include:

- The BADIR Technology Incubators & Accelerators Program, to support the development of entrepreneurship in the technological field.

- The Saudi Research and Innovation Network, otherwise known as “Ma’een,” which links Saudi universities with major international companies and research institutes, providing speed and efficiency in transferring data so that all can benefit from the latest technological advancements — in the Kingdom and around the world.

Last, but by no means least, Saudi Arabia's National Cybersecurity Authority (NCA) hosted the first-ever Global Cybersecurity Forum (GCF) in Riyadh last February. The forum highlighted the Kingdom's efforts to enhance cybersecurity, under the leadership of the NCA and in cooperation with all sectors. The forum also aimed to encourage investment and innovation in cybersecurity and highlighted various national efforts in this sector that contribute to the realization of the Kingdom's Vision 2030 agenda.

Q3. What are some of the key activities your organization has undertaken to enable the government's vision to strengthen Saudi Arabia's cybersecurity outlook?

Cisco's presence in the Kingdom puts security at the heart of Saudi Arabia's digital transformation, as a decisive factor for success. To support the government with its cybersecurity prospects, Cisco announced a series of initiatives to enable the building of a trusted, transparent, and secure digital infrastructure environment.

- Cisco's Country Digital Acceleration Program is a long-term partnership with government, industry, and academia leadership focused on helping the Kingdom achieve its goals of creating a smarter, connected future. As part of this journey, Cisco is working with the government to draft a complete cybersecurity strategy — keeping businesses, citizens, and their data secure.
- Based on its commitment to extending technological solutions to accelerate digitization in the Kingdom, Cisco partnered with National

8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World

Cyber Security Center (NCSC) of Saudi Arabia to upskill their employees in the cybersecurity area through training programs.

- Cisco has built a robust cybersecurity infrastructure for NCSC, and now plans to share its established expertise and deep-rooted knowledge in the service of building new skills and capabilities.
- Cisco's CSR strategic priorities for KSA are human capital development and economic empowerment, focusing on ICT and entrepreneurial skills development through the Cisco Networking Academy program. Cisco NetAcad has trained more than 135,000 students at one of its +100 academies present in the Kingdom.
 - » Cisco NetAcad offer two types of courses: instructor-led and self-pace. Cybersecurity-centric courses have received the greatest interest from students.
 - » Most recently, 15,048 students were trained in cybersecurity.
 - » Female participation in cybersecurity training increased by around 35%.
 - » Cisco is partnering with universities that are advancing their cybersecurity programs and offering such courses as CCNA Security and CCNA Cyberoperation.
 - » Cisco NetAcad will continue to provide training that empowers and upskills students in preparation for the future of work.

Q4. IDC research shows that managing enterprise security is the biggest technology-related challenge for CIOs today. What challenges do you see arising as innovative technologies (like IoT, cloud, artificial intelligence, etc.) drive digital transformation initiatives?

Every day, in every country in the world, security becomes more intertwined with both government and industry, as cyberattacks are increasingly

aimed at jeopardizing critical infrastructures. Such attacks can be launched even from a single home computer.

Successfully preparing for and responding to these modern-day attacks demands a partnership and purposeful coordination between the public and private sectors. Most of all, it requires people to work together, from junior employees to government leaders — and that remains the biggest challenge, because all it takes is one person opening one malicious link to bring down an organization's entire network.

That's why the biggest challenge and most urgent necessity is cybersecurity awareness and training — not just of IT specialists, but of every individual who contributes and has access to an organization's digital property.

Q5. How prepared is the Kingdom when it comes to securing these technologies?

It is clear that the Kingdom is better equipped than most, especially when it comes to capacity building. However, just as new technologies are constantly evolving and becoming more advanced, cyberthreats are too, as hackers change their tactics with greater speed and ease than any organization can update its defenses. That's why even the best antivirus software catches only about 5% of online threats, according to Marc Goodman, cybercrime adviser to both Interpol and the United Nations.

But this does not mean that securing the latest and greatest technologies is impossible; it merely requires security measures that maintain a level of flexibility and responsiveness far exceeding that of even the most persistent cybercriminals.

With its numerous cyberinitiatives, Saudi Arabia is fostering that flexibility and responsiveness; and the more it can continue to do so, the more secure its next-generation technologies will be.

8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World

Q6. What would be key advice for the government to catapult the Saudi cybersecurity ecosystem further into the future?

At Cisco, we believe that a successful cybersecurity approach is built up of multiple layers of protection. In any organization — and especially for government entities — people, processes, and technology must work cohesively to create a strong and effective defense against cyberattacks.

Employees must understand the importance of protecting against cybercrime; meaning that education is key. From simple practices such as using strong passwords to scrutinizing email links and attachments and backing up data, each element helps create an additional barrier against threats. With citizens placing their trust and dependence on the government, the value of each of these simple steps must not be underestimated.

Alongside this, governments must ensure they implement rigid processes with the proper governance to efficiently deal with cyberattacks, which are inevitable. Identifying when an attack is taking place, protecting systems, speedy response and recovery — each element is crucial in building a thorough cybersecurity infrastructure. This is only possible when a unified threat management system is implemented, providing institutions with a holistic overview of their operations, as well as a network that learns and evolves with each threat.

As such, investment in technology is essential for creating an effective layer of protection. Common technologies should be used across the board to protect sensitive data — from endpoint devices such as computers, mobiles, and routers, to networks and the cloud. Solutions include, but are

by no means limited to next-generation firewalls, domain name system filtering, malware protection, antivirus software, and email security solutions.

In today's connected world, no government can afford to be left behind. Citizens rely on the government to deliver services and protect personal data. Entities in Saudi Arabia are embracing digital transformation with open arms, while recognizing the importance of cybersecurity. Every government employee must always be aware, knowledgeable about procedures, and supplied with the necessary resources to ensure that the ongoing digital transformation journey is as smooth as possible.



1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World

9

Cybersecurity and Trust in the Era of Digital Transformation

10. Interview with Al Moammār Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



CYBERSECURITY AND TRUST IN THE ERA OF DIGITAL TRANSFORMATION

Introduction

The digital economy is growing rapidly. According to IDC, the share of worldwide GDP tied to digital services and products will rise from 17% in 2018 to 46% in 2022. A tipping point in the digital economy is fast approaching. Aligned with this trend, organizations' awareness and initiatives pertaining to trust among their ecosystem partners and in their engagements with customers are rising.

FIGURE 9 – Worldwide Nominal GDP (\$ Trillions) Derived from Digital Services and Products



Source: IDC Digital Economy Model, 2019

As organizations, led by their CEOs, become digitally transformed organizations to increase their share of the digital economy, the importance of new agenda items is rising. To validate which new agenda items are rising in importance, IDC conducted a survey among CEOs in the middle of 2019. For each agenda item presented, CEOs were asked whether they believed that item would be more important in the future. As shown in the chart below, 70% of the CEOs believe the following agenda items will be significantly more important for them in the future. "Digital trust programs" were particularly relevant when discussing cybersecurity and digital privacy. This item was cited the most in terms of being likely to increase in importance.

9. Cybersecurity and Trust in the Era of Digital Transformation

FIGURE 10 – A New Agenda for the CEO of the Digital Organization

Q. Please tell us the extent to which you think the importance of each new-agenda item will change over the next 5 years. The answers the figure represents are “more important” and “significantly more important.”



83

DIGITAL TRUST PROGRAMS



76

SOFTWARE CAPABILITIES TO DELIVER INNOVATION



80

INTELLIGENT ORGANIZATION



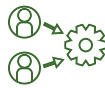
75

EXPERIENCES BUILT AROUND CONTINUOUS CONNECTIVITY



79

NEW INDUSTRY ECOSYSTEMS



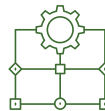
73

DYNAMIC WORK MODELS



77

MARKET-DRIVEN OPERATIONS



71

IT INFRASTRUCTURE RESILIENCY



77

PERSONALIZED CUSTOMER EXPERIENCES

Source: IDC CEO Survey, 2019

Moving digital trust from the CEO's agenda to a bona-fide program will require commitment, and IDC predicts that commitment will be driven not just by the CEO but in concert with the board of directors. By 2025, IDC predicts two-thirds of Global 2000 boards will demand formal trust initiatives to increase these organizations' security, privacy protection, and ethical execution. In putting such initiatives into action, 50% of boards will name a chief trust officer to orchestrate trust across functions, encompassing security, finance, human resources, risk, sales, production, and legal.

Assigning responsibility to a named executive parallels data protection and privacy regulations. The EU's GDPR, for example, stipulates the establishment of a data protection officer (DPO) if personal data processing is a primary operation of the entity. With "personalized customer experiences" as another CEO agenda item of rising importance, personal data processing will be integral to the operations of a growing number of digitally transformed organizations, further adding to their need to establish executive-level and board-reporting accountability.

Challenges in Advancing Digital Trust Initiatives

In executing on their digital trust initiatives, organizations must navigate through several persistent technical and operational challenges in the world of security and trust. Those challenges include:

- A broadening and diversifying IT footprint
- An increasing volume, velocity, and variety of software applications
- Wavering suitability of traditional security measures and delivery methods

The following sections describe the contexts of those challenges.

Broadening and Diversifying IT Footprint

For digital and non-digital organizations, their IT footprints are an expanding and, increasingly, dynamic mix of points of presence. This expansion started at the end of the previous century, when points of presence moved down and out to remote corporate-managed and user-owned personal computers. With the advent of data-supporting mobile networks, smartphones intensified anywhere/anytime connectivity to a new level and thus also the flow of sensitive data and access to corporate systems and applications. The current decade ushered in the cloud era, modifying the concept of a private datacenter from exclusively on premises (i.e., core infrastructure) to essentially anywhere a cloud provider locates its infrastructure.

From this cloud infrastructure, new businesses were born based on the software-as-a-service (SaaS) model, and commercial software consumption evolved from exclusive licensing to a varied mix of licensing and subscription. The spending growth on public cloud services and infrastructure (platform-as-a-service [PaaS] and infrastructure-as-a-service [IaaS]) has been phenomenal. In 2014, worldwide spending was \$66 billion. IDC determined that spending more than tripled to \$229 billion in 2019. Annual spending is expected to double over the next few years, to reach nearly \$500 billion in 2023.

The IT footprint will continue to evolve with increasing expenditure on edge infrastructure as a complement and alternative to core and public cloud infrastructures. IDC predicts that spending on edge compute and storage will grow at a compound annual growth rate (CAGR) of 13.0% from 2019 to 2023 to reach \$21.2 billion in 2023. In comparison, spending on core infrastructure will grow at a 1.1% CAGR over the same period.

Organizations' data assets, systems, and applications are no longer centrally located. The challenge they must confront is how to orchestrate and validate an appropriate level of protection and governance over a highly dispersed IT footprint — one that is also internet accessible.

Increasing Volume, Velocity of Change, and Variety of Software Applications

Consistent with the rising importance of “software capabilities to deliver innovation,” as previously shown in **Figure 10**, the digital organization is increasingly a software development company. Its distinctive products and services and go-to-market approach are traceable to software applications and the data those applications utilize. Consequently, as a critical capability in adapting to changing market and competitive circumstances, the volume, velocity of change, and variety of software applications will increase.

Accordingly, IDC predicts that, by 2025, nearly two-thirds of organizations will be prolific software producers. The percentage of code developers leveraging external software sources (including open source code repositories, services from the major cloud services platforms, platform services from organization

9. Cybersecurity and Trust in the Era of Digital Transformation

app/SaaS providers, and APIs from industry platforms) will thus rise from 30% in 2019 to 80% in 2025. Software development methods and technologies will also change. By 2022, 90% of new organization applications will be developed as cloud-native applications developed with agile methodologies and based on a hyper-agile API-based architecture that leverages microservices architectures, containers, and serverless functions. The development-to-production cadence will also accelerate, with 60% of organizations deploying code to production at least once a day by 2025, up from 3% today. Finally, the developer population will be enlarged and democratized. Additionally, by 2025, organizations will have full-time developer teams that are at least 60% larger than today, and the proliferation of low-code/no-code developer tools will double the population of part-time developers in organizations, such as business analysts, data analysts, and data scientists.

The escalating security and trust challenge for the digital organization is one of secure software code development. If the organization is not already disciplined in secure software code development and applying that discipline within its agile application development workflows, vulnerabilities and sensitive data exposures that the development teams inadvertently build in are sure to multiply.

Wavering Suitability of Traditional Security Measures and Delivery Methods

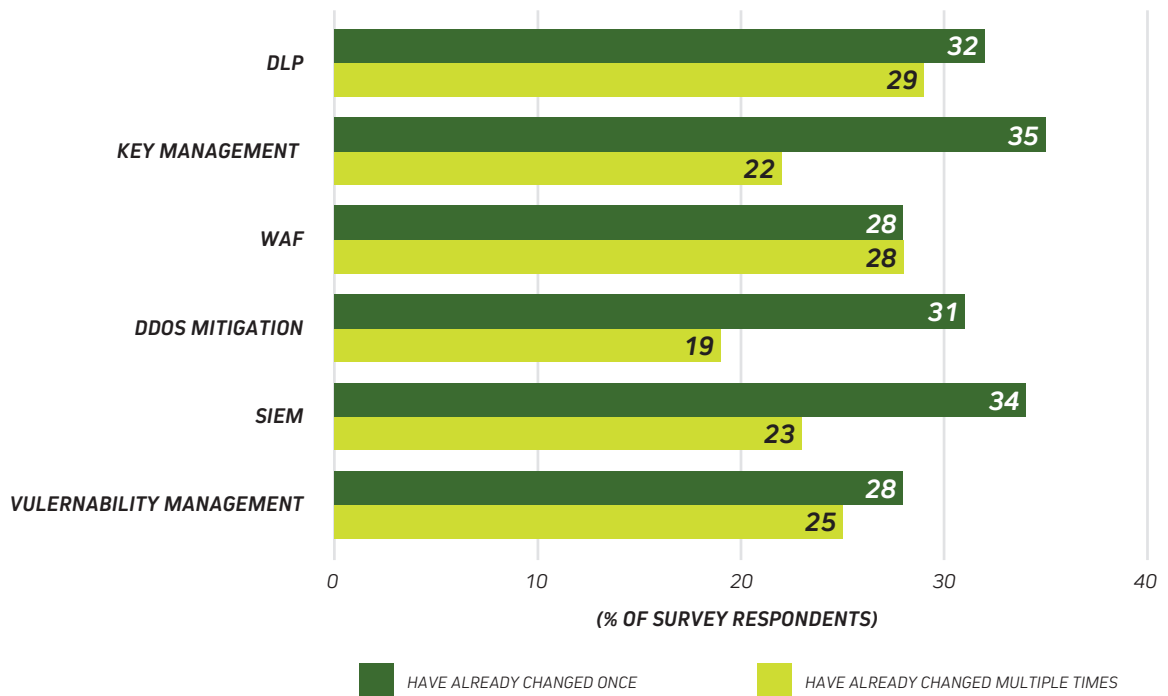
As network- and perimeter-centric security measures have become more permeable to support the agility and openness that digital organizations require, cyberattackers benefit as well. Consequentially, over-reliance on perimeter defenses elevates risk. To counter that risk, digital organizations are evolving their security strategies with greater emphasis on their endpoints, identities, applications, and data as critical security control points.

For organizations that have not adjusted their security strategies to a multi-control point approach, their digital operations are becoming more susceptible to compromise and the risk of sensitive data exposure is increasing. However, greater use of multiple control point security products adds further complexity. This complexity materializes in greater management and oversight of security products and vendor relationships. Also, more control points accentuate the need for skilled staff to orchestrate effective security policies and rules across control points and respond rapidly and with confidence to a potential avalanche of security alerts emanating from those control points.

Extending existing security technologies and products from their original IT environment to another also presents challenges to security efficacy and operational proficiency. Security for cloud instances is a relevant example, whereby extending security products designed for on-premises deployments to the cloud did not universally meet expectations of security professionals. In a late 2018 survey conducted by IDC on the choices made by security professionals in securing their cloud instances, the initial approach was to reuse their on-premises security products. For many of the survey respondents, this approach was short lived, with two-thirds or more of companies changing their cloud security approaches to solutions designed explicitly for cloud use.

9. Cybersecurity and Trust in the Era of Digital Transformation

FIGURE 11 – Frequency of Change in Approach to Secure Cloud Instances



Source: IDC's Cloud Security Survey – North America, 2018

Physical appliances have been part of an organization's security fabric since the rise of the need for cybersecurity. Yet, with growing cloud services adoption and a connected community that is increasingly distributed, the administrative overhead of managing physical appliances and the deployment environment is no longer optimal for organizations' needs.

How Organizations Are Responding

The need to advance digital trust initiatives is real, but so are the previously described challenges. IDC underscores the following developments in security products and markets, with each development sequentially described in greater detail.

- Integrated platforms replacing point products
- The rising adoption of security-as-a-service offerings
- The adoption of security products designed for the IT environments of today
- The use of security virtual network functions in software-defined networks
- The increasing use of managed security services
- Evolution in DevSecOps

Integrated Platforms Replacing Point Products

With the need to apply and enforce security policies at multiple security control points (networks, endpoints, identities, applications, and data), there is also the need to perform multiple security functions at each control point. At the network control point, this functional consolidation has unfolded over the last decade with the creation of unified threat management (UTM) platforms that perform network firewalling, network intrusion detection and prevention, and gateway antivirus. Functional consolidation is progressing in other control points, as well.

At the endpoint control point, this functional consolidation is unfolding between the endpoint protection function and the endpoint detection and response (EDR) function. The benefits from this functional consolidation is a single agent on each endpoint to support both functions and a single administrative interface with role-based access to permit the segmentation of duties among security personnel. Additionally, endpoint protection is expanding in features. Although supported features vary among vendors, common expanding features include application and device control and file-level application whitelisting. In terms of automated identification and blocking of threats, various forms of analytics-based scanning engine have been added to signatures to protect against zero-day threats to keep pace with the onslaught of malware variants.

Another noteworthy development in the endpoint control point is the availability of OS-native security functionality. Microsoft's Defender security suite is one example; another is Chrome OS devices from Google. Both offer a range of built-in endpoint security functions. For some organizations, OS-native security is an attractive alternative to the historical standard approach of third-party OS-overlay endpoint security products. For other organizations, a combination of OS-native and OS-overlay is preferred.

As has historically been the case for most organizations, IT determines the endpoint device strategy (e.g., device makes and models) and security follows with an endpoint security strategy. With endpoint devices equipped with OS-native security, IT and security teams have more reason to develop a joint device and security strategy.

From late 2018 through 2019, several acquisitions of endpoint security vendors by manufacturers of IT equipment occurred. Those acquisitions include BlackBerry of Cylance, VMware of Carbon Black, Broadcom of Symantec, and HP of Bromium. Organizations will likely be presented with more choices in other forms of IT equipment with embedded security capabilities (e.g., endpoint devices with OS-native security by Microsoft and Google) previously accomplished through overlay and network-based solutions.

Data is another control point for which IDC anticipates further functional consolidation. The below table shows the functions and attributes of each function likely to be included in a consolidated data security platform.

9. Cybersecurity and Trust in the Era of Digital Transformation

TABLE 1 – Functional Consolidation in Data Security

Function	Attributes
<i>Data loss prevention</i>	Ubiquitous visibility, control, and protection
	The coalescence of manual classification and the increase of automated classification
	Supervised learning of classifications and tags
<i>File and email encryption</i>	Automated encryption without disruption
	An integrated identity-centric approach
	User-feedback learning
<i>Rights management</i>	File-level granular controls
	Rich telemetry and audit trails
	Employee risk score metrics

Source: IDC, 2020

Rising Adoption of Security-as-a-Service Offerings

Principally spurred by the combination of a distributed workforce and operational footprint and the adoption of software-as-a-service (SaaS) offerings, organizations have come to expect that security vendors provide options to use and manage their security products through SaaS offerings — that is, security-as-a-service (SECaaS). Depending on the organization’s circumstances, a combination of on-premises security control points and SECaaS is used with centralized management applied across both.

Drilling deeper into organizations’ reasons for interest in SECaaS revealed the following:

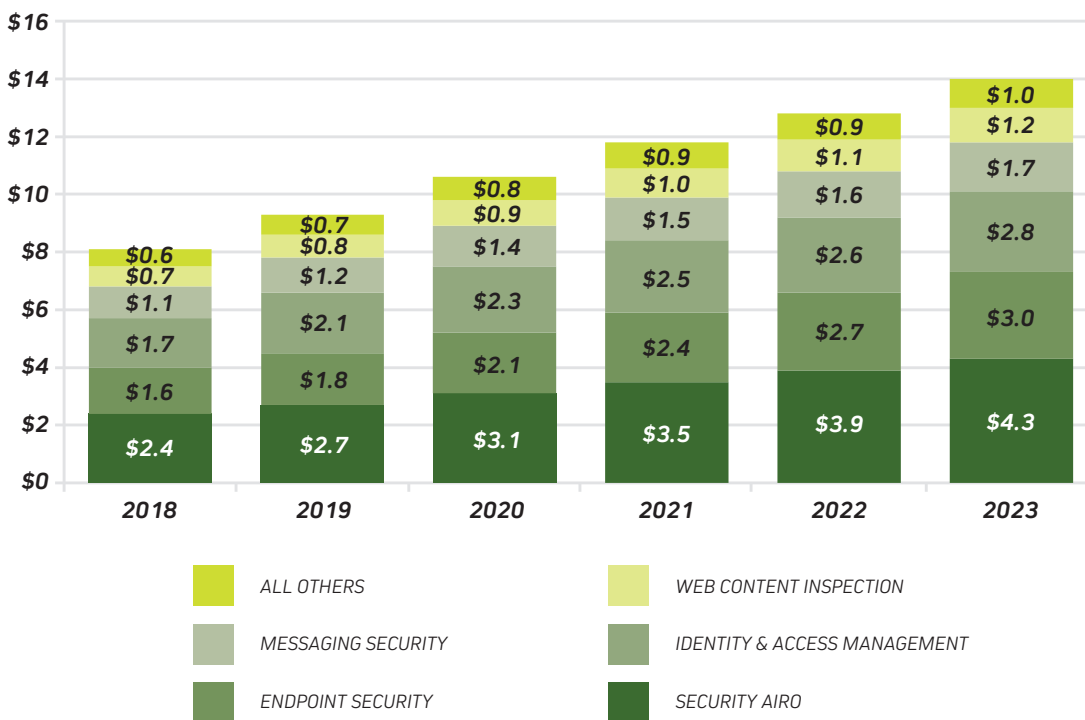
- **Cost effectiveness:** SaaS offerings generally require significantly lower up-front costs than on-premises solutions. In addition, up-front costs for on-premises hardware and software solutions include not only the device itself, but also deployment and configuration. SECaaS offerings typically require none of this, and instead rely on a service contract fee, which covers all aspects of keeping the solution up to date and functioning properly. In addition, on-premises solutions are not free of monthly fees or of their own attached services, often requiring costly service contracts to keep devices up to date and relevant in protecting against current threats.
- **Adoption efficiency:** Adopting new features and functionality, such as distributed denial of service (DDoS) and web application firewall (WAF), can put a significant strain on security personnel and may require system downtime and a lengthy integration process. New solutions require in-depth knowledge of their functionality and configuration, along with detailed knowledge on the existing security infrastructure and how to properly integrate it without redundancies and errors. SECaaS offerings differ in that they will not have to be installed or configured onsite and can be integrated with existing systems with less concerns. This is substantially quicker than deploying on-premises solutions and often far less costly, as well.

9. Cybersecurity and Trust in the Era of Digital Transformation

- **Efficient use of finite resources:** Additional on-premises security hardware and software require trained personnel to install, manage, and maintain the increasingly complex security solution set. This can further inflate the cost of the solution and may not even be feasible given the current shortage of trained security professionals in the industry.
- **Minimized physical footprint:** SECaaS requires no standalone hardware to integrate with existing security infrastructure. However, support of existing components, such as UTM/firewall, is necessary for services to coexist and provide holistic protection across the adopting organization.
- **No upgrade cycles:** As there is no physical device or software installation to upgrade, SECaaS is unique in that it will never require large investments to replace. This also results in significantly reduced strain on security professionals, who would otherwise have to reinstall and configure new appliances or software. For greater agility, selection, staff efficiency, and cost effectiveness, organizations are increasing the use of SECaaS.

Accordingly, IDC predicts SECaaS offerings will grow at a 12% CAGR over the 2018–2023 period.

FIGURE 12 – Worldwide SECaaS Revenue, 2018–2023, Spending (\$ Billions)



Source: IDC, 2020

9. Cybersecurity and Trust in the Era of Digital Transformation

As the circumstances and capabilities around security solutions differ, so too do the reasons that organizations adopt security solutions available through SECaaS offerings. The reasons organizations are adopting identity-as-a-service (IDaaS) include the following:

- To reduce implementation expenditures and extend identity solutions more easily with the following results:
 - » This offers shorter time to value and ensures identity experts, not end-users, do the work.
 - » Single sign-on and multifactor authentication features are readily available.
- To shift complexity of the threat environment to the identity provider by adopting cloud-delivered platforms:
 - » Cloud-based identity providers offer bot management as an essential capability in mitigating credential stuffing threats.
 - » The identity providers are also focusing extensively on DDoS mitigation as customers require always-on availability. A retailer, for example, simply cannot lose availability during peak shopping seasons.
- To support dynamic user populations
 - » IDaaS easily expands and contracts to accommodate the following:
 - i. Elastic support for temporary or seasonal workers
 - ii. Easing the management burden of ever-increasing data sovereignty requirements and corresponding privacy requirements
- To centralize user directories in support of hybrid datacenter environments
 - » To alleviate support calls, IDaaS providers will differentiate on controlling application programming interface (API) drift. Some CISOs report that 80% of support calls are about APIs.
 - » From a best-practices perspective, IDaaS providers will gravitate to using the same APIs internally that outside customers and partners use.

The rate at which organizations are shifting from on-premises to SECaaS also varies among security solutions. For analytics, intelligence, response, and orchestration (AIRO), the economical scalability and extensibility of the SECaaS is driving dramatic shifts in spending on AIRO solutions. In 2014, 4.5% of worldwide AIRO spending was in SECaaS. The relative percentage had increased by nearly 20 percentage points to 24.0% by 2018. IDC predicts this shift will continue, with 56.9% of AIRO spending directed to SECaaS in 2023. Further illustrating this dramatic shift, AIRO spending measured in revenues for SECaaS will increase at a 32.5% CAGR from 2018 to 2023, whereas AIRO spending on on-premises solutions will decrease at a 0.4% CAGR over the same period.

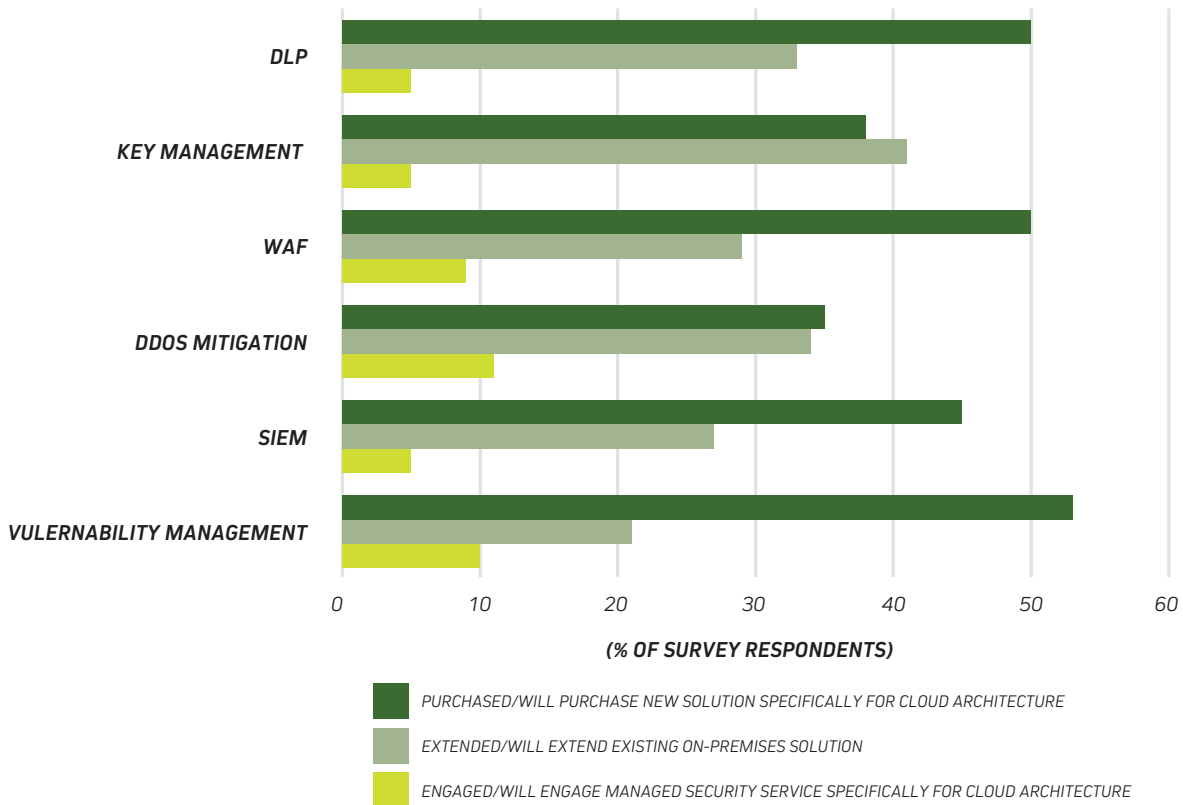
Adoption of Security Solutions Designed for IT Environments of Today

The movement to SECaaS is one case of security solutions evolving to better align with changing customer needs. Another area is in cloud security — that is, protecting IaaS and PaaS instances and securing the data stored and used in these instances. As previously illustrated in **Figure 11**, most organizations have changed their cloud security approach — in some cases, multiple times — since their initial foray into the cloud. Yet, when examining approach changes across security solutions, the variance is notable. As shown in **Figure 13**, most surveyed respondents stated they have, or will be purchasing, new solutions specifically designed for cloud architectures for DLP, WAF, security information and event management (SIEM), part

9. Cybersecurity and Trust in the Era of Digital Transformation

of AIRO), and vulnerability management. For key management and DDoS mitigation, the respondents are evenly split on their preferences for cloud-designed solutions versus extending their existing on-premises solutions. As is also shown, a small percent of the survey respondents stated engaging with a managed security service provider.

FIGURE 13 – *Changed Approaches to Security of Cloud Instances*



Source: IDC’s Cloud Security Survey – North America, 2018

Looking to the future, IDC anticipates that, as cloud-native security services (i.e., security solutions designed for the cloud offered by AWS, Microsoft Azure, and Google) continue to expand and mature, the adoption of cloud-designed security services will increase further. A similar catalyst will unfold as established and new security solution providers introduce and mature their cloud-designed solutions that can be subscribed through the cloud providers’ marketplaces and have cloud-friendly deployment and administrative attributes.

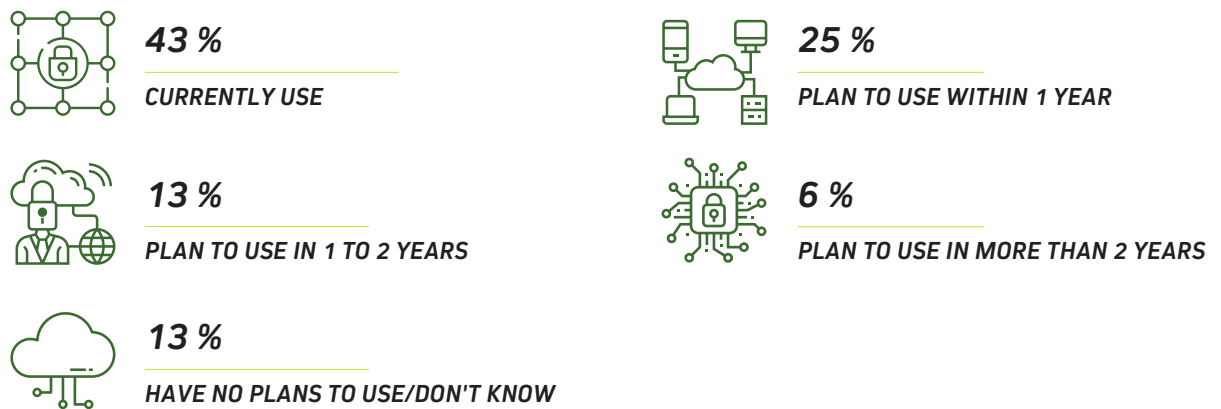
Use of Security Virtual Network Functions in Software-Defined Networks

Another development where security functionality is being used is in the adoption of software defined wide area networks (SD-WANs). Organizations are leveraging SD-WAN platforms to host security solutions configured as virtual network functions (VNFs). SD-WANs with VNFs underlie IDC’s prediction that, by 2023, 60% of organizations will look for integrated solutions with advanced security features, such as embedding automation and intelligence tools, to optimize and secure their core and edge networks.

Demonstrating broad interest in SD-WAN, 87% of organizations that responded to an IDC survey currently use a SD-WAN or are planning to implement an SD-WAN in the future.

9. Cybersecurity and Trust in the Era of Digital Transformation

FIGURE 14 – SD-WAN Adoption in 2019

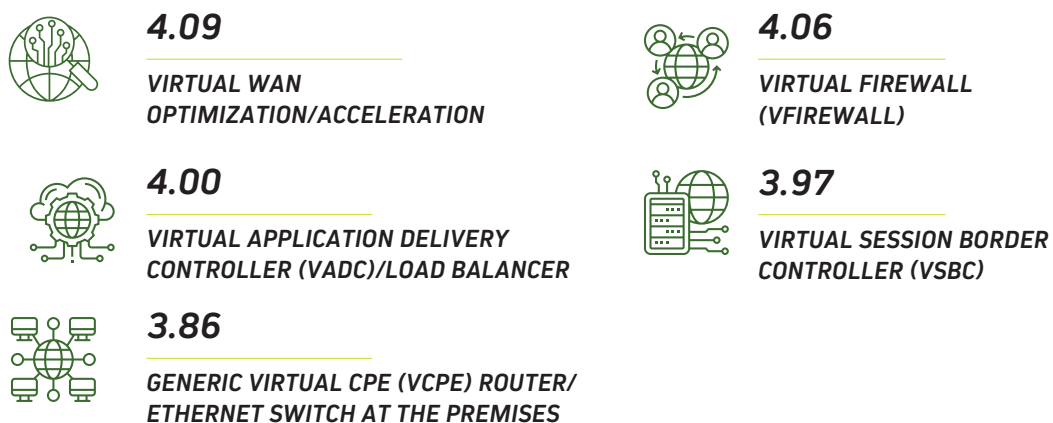


Source: U.S. Organization Communications Survey, 2018

Interest in security VNFs in SD-WAN deployments is strong. Virtual firewalls are among the most likely used VNFs, as shown in **Figure 15**.

FIGURE 15 – Interest in SD-WAN VNFs

Q. Which of the following new virtualized network solutions will you likely consider within the next 12–18 months? Please rate each on a scale of 1 to 5 whereby 1 - 'not at all likely' and 5 = 'very likely'.



Source: U.S. Organization Communications Survey, 2018

9. Cybersecurity and Trust in the Era of Digital Transformation

Increasing Use of Managed Security Services

Organizations are also turning to security service providers (managed, professional, and mixed) to overcome their resource challenges, address the cyber-risks associated with a broadening and diversifying IT footprint, and strengthen their overall security and trust profiles.

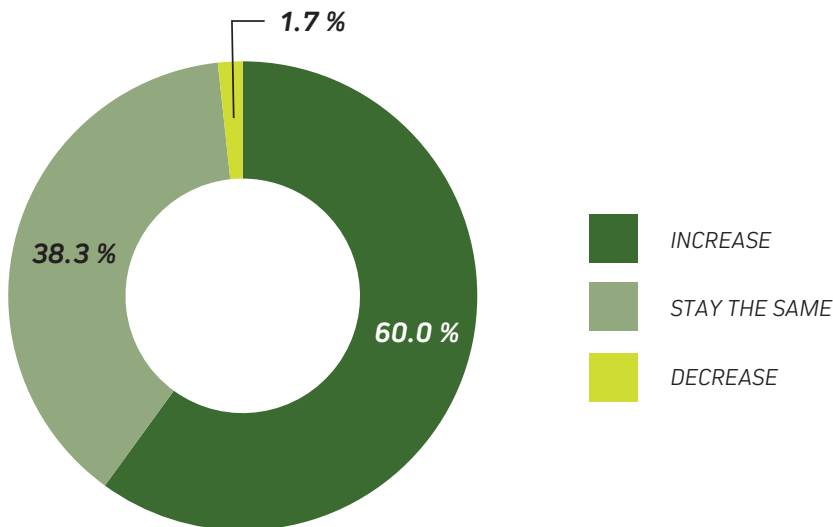
FIGURE 16 – Top Reasons for Using a Managed Security Services Provider



Source: IDC's Managed Security Services Survey, January 2019

According to an IDC survey on demand for managed security services (MSS), the on-going need for MSS is strong, with 98% of surveyed MSS customers reporting they will either increase or maintain their 2018 spending on managed security services in 2019. As shown in **Figure 17**, 60% will be increasing their annual spending.

FIGURE 17 – Changes in Managed Security Services Spending from 2018 to 2019

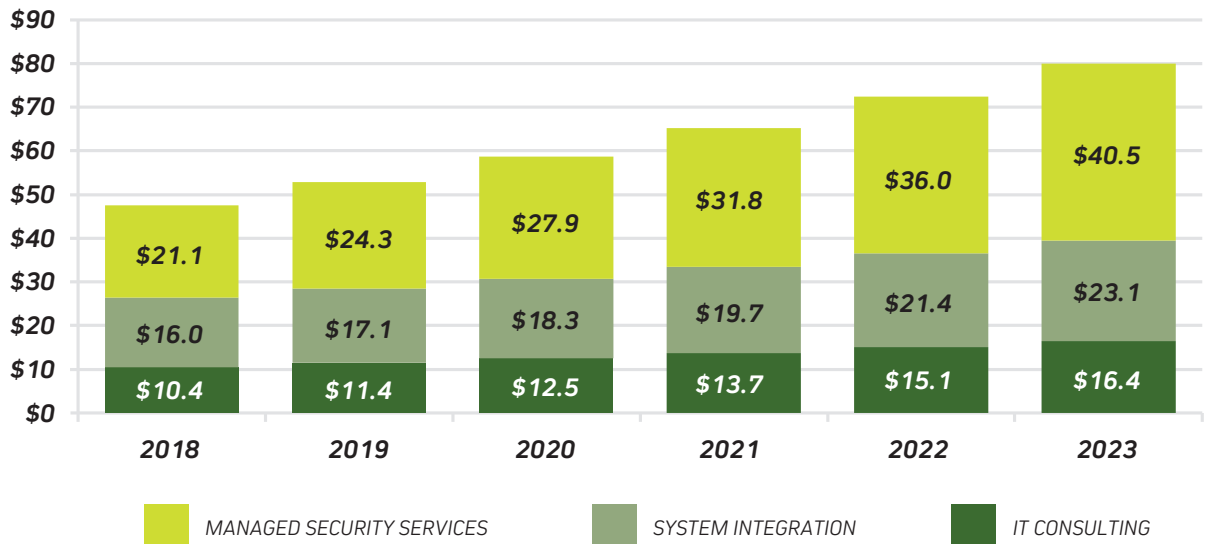


Source: IDC's Managed Security Services Survey, January 2019

9. Cybersecurity and Trust in the Era of Digital Transformation

With the underlying reasons (**Figure 16**) expected to remain in force, IDC predicts worldwide spending on comprehensive security services will grow at a 10.9% CAGR from 2018 through 2023, with spending on MSS growing at the fastest pace — a 13.9% CAGR over the same period.

FIGURE 18 – Worldwide Comprehensive Security Services Spending (\$ Billion), 2018–2023



Source: IDC Worldwide and U.S. Comprehensive Services Forecast, 2018–2023, May 2019

A related development in MSS is managed EDR services offered by EDR product vendors. As with MSS, EDR vendors are finding a growing base of customers seeking external support, from augmentation to full outsourcing, in managing the EDR product, triaging alerts, developing incident response playbooks, executing remediation actions, and conducting threat hunting. IDC anticipates the growing availability of managed services offered by security products vendors in the future.

Evolution in DevSecOps

As previously stated, by 2022, 90% of applications will be developed as cloud-native applications developed with agile methodologies and based on a hyper-agile API-based architecture that leverages microservices architectures, containers, and serverless functions. Combined with an accelerated pace of application development-to-production cadence, security teams operating outside development teams will have been limited to no window of time to erect security and regulatory measures. Worse, their post-deployment security measures could conflict with the application's functionality or performance or both.

With this future view, IDC anticipates that the development, operations, and security teams within most organizations will collaborate at a greater level than now. This collaborative movement is aptly named DevSecOps.

However, the degree to which these separate teams collaborate will not be uniform. Variation across organizations will be influenced by culture, leadership, and risk tolerance. Additionally, tools that, 1) facilitate cross-team collaboration or mitigate occurrences of risky code inserted during development

9. Cybersecurity and Trust in the Era of Digital Transformation

(e.g., excessive permissions, configuration errors, insertion of untrustworthy code, and APIs with risky resources), 2) assess risk-producing drift in assembled code, and 3) audit risk during runtime, will also have a material bearing on the progress of the DevSecOps movement.

Beneficially, DevSecOps tools are coming to market in three vectors. Those vectors are cloud-native, start-ups, and established security vendors.

- **Cloud-native:** The prominent public cloud providers — AWS, Microsoft Azure, and Google Cloud Platform — have been building, and continue to build and mature, cloud-native security development tools, security monitoring and reporting capabilities, and response mechanisms.
- **Start-ups:** Since its inception, the cybersecurity industry has been one of continuous funding for start-up launches and commercialization. Over the last half decade, a portion of that funding has been directed at start-ups aimed at addressing the security risks associated with cloud adoption and the risks associated with cloud-native agile software development.
- **Established security vendors:** Mindful of the evolving and expanding IT footprint in the cloud, SaaS offerings, and agile software development, established security vendors have been active acquirers of cloud security start-ups. Cloud security acquisitions by Splunk (SignalFX and Omnitron), Palo Alto Networks (Twistlock and PureSec), and Check Point (Dome9 and Protego Labs) — all in 2019 — are relevant examples of established security vendors broadening their portfolios to support their customers' cloud security needs and DevSecOps teams.

As this latest wave of DevSecOps is in its nascent stage, IDC expects that new and enhanced DevSecOps tools will continue to flow into the market over the foreseeable future.

Conclusion

As organizations pursue digital transformation, their approaches to cybersecurity and digital trust must be foundational. The historical approach of bolting on security once the IT infrastructure is in place has proven to be an inadequate defense against the myriad of cyberthreats organizations face. Moreover, as the pace of change for digital organizations accelerates, a bolt-on approach will perpetually be reactive and leave windows of vulnerabilities open for attackers to exploit. As a result, the frequency and severity of system compromises and data breaches will intensify.

As buyers of technology that directly contribute to cybersecurity and digital trust, buyers have several directional choices ahead. IDC's guidance is summarized in the following three statements.

- **Assess and aim. Cybersecurity and trust are objectives with constantly changing end states.** What defines a secure environment today is different tomorrow, and the same goes for trust. Therefore, each organization that is serious about cybersecurity and trust must first objectively benchmark its current state of cybersecurity and trust to industry norms and internal expectations. Holistically is best, but a pragmatic approach focusing on specific areas, such as data privacy and protection, identity and access management, or incident detection and response, may be more realistic. Once the current state is determined, a gap analysis follows covering what the gaps are and the severity of each. While it seems compelling to jump in and fix right away, deciding where to aim is critical. For example, an organization that defines cybersecurity and trust as strategic to its business will have a different aim than one that views cybersecurity and trust as a supporting element of its business. Once this assess-and-aim exercise is done, planning and execution come next. Finally, as changing end states is a given, assessing and aiming must be a recurring and routinized exercise.


9. Cybersecurity and Trust in the Era of Digital Transformation

- **Build a community of committed stakeholders.** The pervasiveness of cybersecurity and trust impacts all departments and employees within your organization, along with your customers and business partners. Finding stakeholders with opinions on issues and objectives is easy. Finding stakeholders that are committed, enabled, and accountable to drive resilient and structural improvements in cybersecurity and trust is a more difficult challenge. Nevertheless, this is a challenge that should be taken with unrelenting vigor. Only with a community of committed stakeholders will steady and measurable progress materialize.
- **Lean heavily on your cybersecurity and trust solution providers.** Leaning is not synonymous with relying. The marketplace of cybersecurity and trust solution providers is vast and innovative. Therefore, buyers should not hold back on leaning hard on this marketplace to deliver what they need now and in the future. It is also important to recognize that effectiveness in leaning hard to get one's needs met is gated by knowing where one is and where one is going (assess and aim) and having committed stakeholders in place. Certainly not all organizations are this mature in their approach to cybersecurity and trust. At the same time, decisions on which vendors' solutions to use must be made. To assist navigating this decision tree, we believe organizations should assess three attributes in making any cybersecurity and trust solution and provider selection. Those attributes are interoperability, adaptability, and scalability.

1. Saudi Arabia's Cybersecurity Landscape
2. Interview with Saudi Information Technology Company (SITE): Advancing the Kingdom's Cybersecurity Landscape
3. Evolving Competitiveness of the Local Cybersecurity Ecosystem
4. Interview with Trend Micro: Setting Up Smart Cybersecurity for an Evolving Threat Landscape
5. Initiatives & Developments to Improve the Saudi Cybersecurity Environment
6. Interview with Mobily: Securing the Kingdom's Digital Transformation Journey
7. Cybersecurity Challenges in Today's Digital World
8. Interview with Cisco: Enabling Cybersecurity in an Increasingly Interconnected World
9. Cybersecurity and Trust in the Era of Digital Transformation

10

Interview with Al Moammār Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic



10. Interview with Al Moammad Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic

ZIAD MORTAJA

CEO, Al Moammad Information Systems (MIS)



Ziad Mortaja is the CEO of Al Moammad Information Systems (MIS). During the pandemic, he managed to lead one of the largest system integrators in the KSA in one of the most challenging situations facing the economies. Managing over 700 technical experts remotely during the quarantine, while driving the company's growth and delivering landmark projects to key entities in the Kingdom of Saudi Arabia. Mortaja has proved to be an experienced leader with in-depth knowledge of the Saudi market, showing an exceptional performance during the crisis.

With over 33 years of experience in the ICT and energy sectors in the Middle East and Australia, Mortaja brings a fresh perspective to MIS and alignment to the KSA Vision 2030 and NTP programs. Before joining MIS, Mortaja was the country manager of Schneider Electric in KSA.

Before that, he served as managing director of Hewlett Packard (HP) Saudi Arabia and later as senior director of the Networking Division for the Middle East, Mediterranean, and Africa. Prior to HP, Ziad spent 10 years at Cisco Systems in Saudi Arabia, then in North Africa and the Levant, where he was the director and general manager of the region.

Ziad holds a bachelor's degree in Computer Science and Software Engineering from Kuwait University. He was also awarded several certifications in Leadership, Management, Finance and Business from internationally recognized centers.

10. Interview with Al Moammar Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic

Q1. How would you describe the importance of cybersecurity in the context of the economy lockdown, especially with the growing sophistication of cyberthreats and the need to gradually resume business activities?

Cybersecurity has proven that it is one of the “must have” components within the ICT infrastructure. It is not required to fulfill the Kingdom’s 2030 vision only, it is now the most important part to enable organizations to work remotely with full protection to its connectivity and digital assets during the pandemic. It should precede the execution of any project, since it is much easier to secure the digital system during the planning phase, while it is almost impossible to secure a poorly designed network and eliminate all the backdoors that can be used by hackers to initiate cyberattacks.

Q2. With the public sector at the helm of digital transformation in the Kingdom, what is your view on the various initiatives that the Saudi government has launched in order to improve the local cybersecurity landscape?

The Saudi government launched many initiatives a long time back to strengthen the Kingdom’s cybersecurity infrastructure and protect the crucial facilities against any data breach or denial of service. However, a major achievement in 2019 was escalating the role of the NCA through an important engagement within the government sector for enforcing regulations, standards, and conducting a total review of the cybersecurity capabilities within ministries and governmental agencies.

Also, I believe that establishing the Saudi Authority for Data and Artificial Intelligence will have a strong impact on the Kingdom’s cybersecurity capabilities. This will enable Saudi Arabia to deploy more advanced security systems empowered by machine learning and artificial intelligence. Furthermore, it will assure better integration and protection of sensitive data in both the public and private

sectors. This step, the deployment of Artificial Intelligence Security Systems that can track trends and analyze user behaviors, will make it almost impossible for hackers to succeed in their attacks, which are usually based on security limitations in certain components within the network.

Q3. What are some of the key activities your organization has undertaken to enable the government’s vision to strengthen Saudi Arabia’s cybersecurity outlook?

We are providing key government entities with innovative solutions and state-of-the-art products developed by global cybersecurity leaders to strengthen their information security infrastructure and data protection capabilities. We also conduct many training sessions and participate in leading security events, where we share our know how and exchange information with key cybersecurity players in Saudi Arabia.

Q4. IDC research shows that managing enterprise security is the biggest technology-related challenge for CIOs today. What challenges do you see arising as innovative technologies (like IoT, cloud, artificial intelligence, etc.) drive digital transformation initiatives?

New technologies are creating a major disruption across the ICT landscape. The main challenge we are facing now is rectifying skills shortages, either for administrators for the new systems or as end users. Moreover, the interconnectivity between personal and corporate devices adds complexity to the IT environment. At the same time, the market lacks an end-to-end cybersecurity solution, which complicates the job of IT administrators by forcing them to deploy multiple system from different vendors.

Traditional government agencies lack the cybersecurity capacity to react effectively to new forms of proliferating attacks, as hackers exploit

10. Interview with Al Moammar Information Systems (MIS): Developing Capabilities for Addressing Cybersecurity to Enable Business Continuity During the Pandemic

the vulnerabilities created by new technologies like IoT and cloud, while enhancing their own attack techniques with artificial intelligence. That's why we are working closely with government agencies and the Saudi cybercommunity to develop a new approach to attacks and stay one step ahead of hackers.

Q5. How prepared is the Kingdom when it comes to securing these technologies?

Saudi Arabia is ranked 35 globally as per the National Cyber Security Index (NCSI), which indicates that the Kingdom is well prepared in regard to cybersecurity technologies. We are confident that many projects and plans are under development to assure that Saudi Arabia will be among the top countries in the area of cybersecurity. MIS is prepared to join these efforts through the partnerships we have with the leading information security vendors worldwide. However, with the recent impact of COVID-19 on the way we are doing business, I believe the government will allocate more capabilities and resources in cybersecurity, to allow end-to-end online transactions and user experience.

Q6. What would be key advice for the government to catapult the Saudi cybersecurity ecosystem further into the future?

Most importantly, Saudi talent should be involved at the core of the R&D process of cybersecurity, including full access to source codes and encryption algorithms, to ensure that the Kingdom's cybersecurity requirements are fulfilled. In addition, mobile apps and social media need to be more strictly regulated, as they are attractive for hackers due to lack protection of personal data. Finally, a massive awareness campaign should be initiated to educate people against cyberattacks.

IDC Team



Michael Suby
Research Vice President
Security & Trust



Craig Robinson
Program Director
Security Services



Uzair Mujtaba
Program Manager
Services – Saudi Arabia



Sourav Bhanja
Director
Consulting – Middle East & Africa



Hamza Naqshbandi
Regional Director
Saudi Arabia & Bahrain

IDC Saudi Arabia

Office #401, 4th Floor, Gate A1
Riyadh Gallery Mall
Imam Saud Bin Abdulaziz Bin Mohamed Road
King Fahd District
P.O. 18648, Riyadh 12262
Saudi Arabia

Tel: +966 11 275 6117

Twitter: @IDC

www.idc.com

Copyright Notice:

External Publication of IDC. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC vice president or country manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason. Copyright 2020 IDC. Reproduction without written permission is completely forbidden

Prepared by:



Sponsored by:



884.60

773.9 365