Oman's Cyber Security

And the National Programme for the Development of the Digital Economy

Kifah Al Mahruqi

OBBC

THE ANGLO-OMANI SOCIETY
الجمعية البريطانية العمانية

In October 2021, the Council of Ministers approved the National Programme for the Development of the Digital Economy. This strategy aims to build a thriving digital economy and is aligned with the goals and objectives of Oman Vision 2040. It also identifies a number of foundations that will lead to the building of the digital economy through a series of medium and long-term goals that aim to develop a comprehensive digital infrastructure, establish e-commerce and build a digital workforce. Overall, this will empower and stimulate various economic sectors including education, tourism, logistics and manufacturing.

Amongst the medium-term goals identified in the programme is cyber security – a clear indication that leaders recognize that cyber security is a prerequisite building block that has a significant impact on the economy and will allow new opportunities to be explored in the ever-growing need for cyber security products, services and skilled labour force. The rate of growth in the cyber security industry doesn't appear to be slowing down. As we become even more digitally advanced, we are experiencing higher rates of cyber crimes and incidents, meaning we require an ever-growing number of professionals to deal with increasing threats. The skills gap is often so large that companies are willing to hire employees from a non-cyber security background with unrelated degrees, as long as they have some form of experience or certification and exhibit eagerness to learn.

Kifah Al Mahruqi

Lead Governance, Risk Assurance Analyst, & SAP Architect,

Petroleum Development Oman

Oman is aware of the importance of cyber security to the economy, not just locally, but as a country with a significant presence in the region that must protect its Critical National Infrastructure (CNI). On a national level, incidents are on the rise targeting government and CNI sectors such and the energy and banking industries. Incidents have mainly focused on intrusion attempts, malicious code, malware infection, web phishing and ransomware as the top types of attacks targeting CNI. These attacks not only aim to destroy data and availability of services, but to potentially sabotage an organisation's operations and trigger explosions which may lead to loss of human life.

With challenges come opportunities and this includes the various ways that the Covid-19 pandemic has influenced the cyber security landscape. The pandemic has accelerated the adoption of digital technology in both private and public sectors and evidently those

technologies have become vital to societies. Working from home was not even a remote possibility in most organisations in Oman – both public and private sectors –and overnight a complete shift and rush to embrace digital tools occurred. This has heightened our dependence on internet-connected technologies and cyber criminals have shifted their focus accordingly to exploit that dependence. Despite the potential vulnerabilities inherent in the digital space, it has been very encouraging and positive to observe the pace and acceptance with which a robust, digital infrastructure was rolled out during difficult times in the early weeks of the Covid crisis. The pandemic also helped raise awareness, amongst government and business leaders, of the global interdependence on the internet and the importance of cyber security investments to provide an assurance that businesses can continue to operate under such circumstances.

There has also been a widespread realization that e-transformation is not a nice, convenient service but a must-have for the economy's success and survival. With the growth of cloud services, e-commerce and almost universal smartphone use, Oman must seize the opportunities provided by the latest ICT developments and rise to the occasion when it comes to overcoming challenges as new opportunities bring new risks, particularly in cyber security. Preventing these risks

"There has also been a widespread realization that e-transformation is not a nice, convenient service but a must-have for the economy's success and survival."

is something Oman has prepared and set the foundation for. In the latest UN Global Cybersecurity Index, Oman was ranked third in the Arab world and 21st globally as being prepared to deal with cyber crimes in the Global Cybersecurity Index 2020 report. Having a comprehensive and coordinated cyber security strategy has been crucial in defending the country against attacks which will in turn help enhance the ICT sector, as a good security record is essential to becoming a technology hub.

It is expected that the National Programme for the Development of the Digital Economy with all its components, such as innovation and smart e-government, will build on previous efforts to realize national goals and KPIs - the most important one being contribution to the national GDP as we diversify away from reliance on oil. Economic investment will increasingly be dependent on how well we, as a country and

as organisations, can demonstrate that we do indeed have a secure digital infrastructure and a secure cyberspace. This includes the ability to attract foreign investments and expertise, making it easy for startups and established businesses to set up shop and be able to operate without jumping through many bureaucratic hoops. It requires national policy frameworks which focus on mitigating risks without hindering the vast promise of emerging technologies such as blockchain and artificial intelligence, whilst building national capabilities and skills that will also provide employment and entrepreneurship opportunities.

To ensure the success of cyber security in organisations, security professionals need to focus on developing timely responses to incidents and be able to handle unexpected events with minimal impact on the business whilst maintaining situational awareness. Having an up-to-date and refreshed security infrastructure strategy is crucial as outdated, fragmented security infrastructure hinders the organisation rather than acting as an enabler that brings value and efficiencies. This does not mean organisations need to replace everything all in one go but instead, they must prioritise and make assessments based on risks. This will prevent a lot of security issues that are a result of legacy

Kifah AlMahruqi, Cybersecurity Panel at UK Oman Tech 21

software and hardware.

Involving senior management in conversations about cyber risk, and its business impacts, can ensure the entire organisation buys into security efforts. I believe most organisations should include cyber security in their corporate risk profile and board decisions but traditionally, this hasn't been easy. The Security Operations Center (SOC) may not speak the same language as the C-Suite or board. That's because security managers and staff tend to focus on the technical aspects of managing cyber risk and incidents while executives and board members want to know the financial impact of a cyberattack or the reputational damage if classified data is leaked or customer data is stolen. By quantifying cyber risk in financial terms or potential regulatory consequences,

executives and board members can better understand what kind of hit the company might take if it's the victim of a ransomware attack or other threat.

The need is therefore to remain diligent as individuals, staff, leaders, organisations and policy makers so that there is an effective first defence against attacks and a chance to stop them from happening. In an ever-connected ecosystem of networks and devices with a wider attack surface where criminals are constantly more sophisticated and motivated than the defenders, we must all work together to mitigate these risks and also work towards creating trust for a robust cyber security ecosystem in Oman that supports the growth of our digital economy and the objectives of Oman Vision 2040.