The State of Cyber (In)security in the United Arab Emirates

Hande Guven

May 07, 2018

Abstract

Although until recently cybercrime and risk of data theft were considered to be issues faced by developed nations, as digitization in both governance and business rises, Middle East countries are also beginning to realize the importance of cybersecurity readiness. The United Arab Emirates is one of the biggest economies in the region and one of the top countries in the world in terms of digital consumer adoption. These qualities, coupled with insecure consumer habits and lack of adequate cybersecurity measures in key sectors, make the UAE an alluring target for cyber attacks. This paper examines the level of cyber preparedness and security measures using three metrics: 1) cybercrime and its effects on the economy 2) human attack surface of cyber threats, 3) the state of national cybersecurity strategy.

1. Introduction

Middle East — a rapidly digitizing region with an estimated population of over 411 million[1] — is home to an increasingly complex cyber threat ecosystem. Although until recently cybercrime and risk of data theft were considered to be issues faced by developed nations, as digitization in both governance and business rises, Middle East countries are also beginning to realize the importance of cybersecurity readiness. Despite the progress made by several countries in recent years, a variety of structural shortcomings — lack of efficient legislative and regulatory frameworks and inadequate cybersecurity workforce — limit the scope of progress and expose countries to cyber risks. According to the 2014 Microsoft Security Intelligence Report computers are becoming infected in the Middle East at increasingly higher rates than the global average[2] with developing nations in the region are particularly vulnerable to cyber threats.

According to a 2014 report, cybercrime is estimated to cost the global economy a reported US$400 billion annually[3] with costs predicted to rise to $6 trillion annually by 2021.[4] For perpetrators of such crime, The Middle East is a particularly desirable target because of a combination of factors: poor security awareness of many ICT users, the shortage of technical ability to defend systems and the lack of appropriate legislation.[5] Furthermore, the rapid rate of digitization across the region contributes to the increased attack surface and prevalence of systems underqualified to defend against attacks. According to PricewaterhouseCoopers report, companies in the region suffered much larger losses than other regions in 2016, as a result of cyber incidents: "56% lost more than $500,000 compared to 33% globally, and 13% lost at least three working days, compared to 9%."[6] As such it is important to understand the different challenges faced by countries in the region and measures taken to defend against cyber attacks.. This paper will examine the state of cyber insecurity in the Middle East by looking at the United Arab Emirates, a regional leader of digitization..[7]

---

[1] "The Middle East Population 2018." *The Middle East Population 2018 (Demographics, Maps, Graphs)*, worldpopulationreview.com/continents/the-middle-east-population/.
[2] Ibid.
[3] https://www.gcsp.ch/download/6791/159595
[4] Morgan, Steve. "Top 5 Cybersecurity Facts, Figures and Statistics for 2018." CSO Online, January 23, 2018. https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html.
[5] El-Guindy, Mohamed N. "Middle East Cyber Security Threat Report 2014." Accessed May 8, 2018. https://www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014.
[6] PricewaterhouseCoopers. "A false sense of security?: Cybersecurity in the Middle East" Accessed May 8, 2018. https://www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf
[7] Elmasry, T., Benni, E., Patel, J. and aus dem Moore, J. P. (2016), Digital Middle East: Transforming the region into a leading digital economy, McKinsey & Company, October 2016, https://www.mckinsey.com/~/media/mckinsey/global%20themes/middle%20east%20and%20africa/digital%20middle%20east%20transforming%20the%20region%20into%20a%20leading%20digital%20economy/digital-middle-east-final-updated.ashx

This paper will aim to answer a simple yet multifaceted question: how big the problem of "cyber insecurity" in the context of the Middle East? In particular, this paper will define and examine several metrics in order to accurately evaluate a state's cyber readiness and maturity levels. These metrics include (1) cybercrime rate and its effects on the economy, (2) human attack surface of cybercrime (3) cybersecurity policy and strategy.

2. To the Community

Although cybersecurity is becoming an increasingly crucial area of discussion and political scientists are beginning to take note of the cyberspace as a political realm there is still relatively few academic texts on the subject. In fact readers of this report will find that an overwhelming portion of the sources cited are news articles or evaluations produced by private sector leaders including management consulting and cybersecurity firms. It is even less common to find resources focusing on specific issues and regions such as developing countries and the Middle East. This is one of the reasons why looking at the state of cybersecurity readiness in the Middle East is a significant undertaking. With rapidly digitizing commercial and public sectors, a significant demographic of young people and a complex web of political relations the region serves as a hotbed of cyber activity, both from profit-motivated and government actors. As such, this paper will aim to shed light on the levels of cyber readiness in one of the digital leaders of the region, the United Arab Emirates.

3. United Arab Emirates

The United Arab Emirates is one of the biggest economies in the region with a gross domestic product (GDP) of more than $690 billion.[8] Although UAE has one of the most diversified economies among Gulf countries, it remains heavily reliant on oil exports. In terms of digital consumer adoption, the United Arab Emirates is one of the top countries in the world with more than 100 percent smartphone adoption and more than 70 percent social media use — figures that are even higher than the United States.[9]

Digitization Facts and Figures:

- Population: 6,072,475
- United Nations E-Government Index Ranking: 29
- Mobile-cellular subscriptions per 100 inhabitants: 214.7
- Households with Internet access at home (%): 94.3
- Individuals using the Internet (%): 90.6

[8] "The World Factbook — Central Intelligence Agency." Accessed May 8, 2018. https://www.cia.gov/library/publications/the-world-factbook/geos/ae.html.
[9] McKinsey & Co. "Digital Middle East: Transforming the region into a leading digital economy" Accessed May 8, 2018. https://www.mckinsey.com/~/media/mckinsey/global%20themes/middle%20east%20and%20africa/digital%20middle

Similarly according to 2016 McKinsey report, the UAE government ranks number in digital adoption rates across the region with expanded broadband access and a newly-unified smart city platform.[10] The same McKinsey paper reports high digitization among consumers, businesses and government in the United Arab emirates. As part of the UAE Vision 2021, the National Innovation Strategy declared digital technology as a top primary national sector with plans to develop advanced technologies including smart cities.

But why does increased digitisation a cause of worry? As exemplified by the wave of ransomware attacks in 2017, securing systems is a complex overtaking and with rapid digitisation comes vulnerability. The question is whether the UAE is prepared to simultaneously secure its systems and push for a country-wide "digital transformation."

a) Cybercrime in the UAE

While reliable and accurate data from official sources regarding the rate of cybercrime in the United Arab Emirates is difficult to find, news pieces on waves of debilitating malware attacks and research by private companies reveal the magnitude of the problem to some extent.

For the purposes of this research paper the term "cybercrime" is defined as crimes that fall under at least one of the following criteria: crimes 1) that target and tarnish the confidentiality, integrity and availability of computer systems and data 2) in which the computer is used as a weapon (e.g. distributed denial of service (DDoS) attacks). Examples of cybercrime include network intrusions, phishing, viruses, worms and malware. F

Symantec's Cybersecurity Insights Reports reveal that the financial cost of cybercrime increased from USD $1.3USD in 2015[11] to $1.4 billion in 2016.[12] Tamim Taufiq, head of Norton Middle East, credited the 4.9 percent increase to the UAE becoming an ideal target for cybercriminals because of 1) high penetration rates of smartphones 2) adoption of new technologies 3) the high profile the country has internationally.[13] Keeping in line with the trend of rising financial damages associated with cyber crime, Symantec estimates that the average amount of time

%20east%20transforming%20the%20region%20into%20a%20leading%20digital%20economy/digital-middle-east-final-updated.ashx.

[10] Ibid.

[11] Symantec. "Norton Cybersecurity Insights Report 2015." Accessed May 8, 2018. https://ae.norton.com/norton-cybersecurity-insights-report-uae.

[12] Symantec."2016 Norton Cyber Security Insights: The UAE" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-comparisons-uae-en.pdf.

[13] Gulf Business. "Six Arrested In $45m Global Cybercrime Involving RAKBANK, Bank Of Muscat" Accessed May 8, 2018. http://gulfbusiness.com/six-arrested-in-45m-global-cybercrime-involving-rakbank-bank-of-muscat/.

consumers in the UAE lost dealing with the impact of online crime rose steadily from 30 hours in 2016 to 47.5 hours in 2017.

Similarly, according to Kaspersky Lab's statistics, United Arab Emirates ranked 8th globally in 2016 in the percentage of users attacked by banking Trojans. One of the most common types of financial cybercrime, banking trojans are constantly evolving with new versions joining the ranks of existing malware every day.[14] Kaspersky reports that the five of the top 10 banking Trojans in 2016 targeted smartphones running Android OS. This is especially significant for United Arab Emirates with more than more than 100 percent smartphone penetration.[15] Even more alarming is the fact that Android is the operating system with the highest market share in the United Arab Emirates with approximately 40% of the market under its control. This goes to show that cybercriminals are keeping track of consumer trends and changes in user behavior to finetune their attack strategies. Credit/debit card fraud was the most costly cybercrime method in the UAE in 2017 with more than $1000 lost per consumer.[16]

In addition to individual users, financial institutions and government agencies were also hit hard by cybercrime, specifically targeted attacks including DDoS attacks and malware infection. For instance, the UAE was hard hit by cyberattacks against the financial sector in 2013. Furthermore, malware infection were the most common cybercrime experienced in the UAE in 2017 with more than half of all incidents stemming from malware.[17] The largest cyber attack in the region to date targeted two banks in the region: the National Bank of Ras Al-Khaimah RAK) in the UAE and Bank Muscat in Oman in two attacks in December 2012 and February 2013. The two attacks combined stole more than $45 million from the two banks[18]. Following the incidents, RAKBank came under fire from customers for not disclosing the attack and the consequent monetary damage in a timely fashion.[19] RAKBank waited five months to acknowledge and disclose the attack to the public while Bank Muscat disclosed the news in the days following the incident.

According to Verisign — an internet infrastructure company that operates two of the internet's thirteen root nameservers— the first quarter of 2017 saw a 23 percent decrease in the number of

---

[14] Garnaeva Maria et al. Kaspersky Labs. "Kaspersky Security Bulletin: Overall Statistics For 2016" Accessed May 8, 2018. https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf
[15] Ibid.
[16] Symantec."2017 Norton Cyber Security Insights: The UAE" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-uae-en.pdf
[17] Ibid.
[18] Gulf Business. "Six Arrested In $45m Global Cybercrime Involving RAKBANK, Bank Of Muscat" Accessed May 8, 2018. http://gulfbusiness.com/six-arrested-in-45m-global-cybercrime-involving-rakbank-bank-of-muscat/.
[19] The National. "RAKBank comes under fire from customers over cyber attack." Accessed May 8, 2018. https://www.thenational.ae/business/rakbank-comes-under-fire-from-customers-over-cyber-attack-1.260919

DDoS attacks in the UAE while the average peak attack size increased 26 per cent.[20] In terms of ransomware, the UAE got off relatively scot-free from the 2017 WannaCry attacks because it took place on a Friday, which is a non-working day in the UAE as well as some other majority Muslim countries in the region.[21] Official sources state that there were no confirmed cases of Petya infection either, therefore it is difficult to quantify the financial effect of the recent waves of ransomware attacks.

b) Human attack surface

The United Arab Emirates, much like the rest of the Gulf region, has a significantly young population with a median age of 30 years[22] which results in a cohort of tech-savvy digital users and consumers. While this attribute results in high digital penetration rates and facilitates the UAE government's digital transformation efforts, it also results in a larger section of the population being vulnerable to cybercrime. Data from Symantec shows that the total consumers in the UAE affected by cybercrime rose from 2.5 million people in 2016[23] to 3.72 million in 2017, which means more than half of the population experienced cybercrime in 2017.[24]

As mentioned before, one of the biggest drivers of digital transformation in the UAE is the large cohort of young people, some of whom are digital-natives, who feel significantly more comfortable with technology than their predecessors. While their online habits are driving consumer trends and fueling rapid digital penetration, they remain vulnerable to cybercrime. According to data by Norton Cyber Security Insights Report, millennials in the UAE are far more likely to experience cybercrime than other age groups as a result of their increased connectivity.[25] This holds true across globe: Millennials own the most devices (four devices on average) and have the least amount of cyber hygiene: one in four of Millennials use the same password for all accounts and 63 percent have shared at least one of their passwords with another person.[26]

---

[20] Gulf Business. "DDoS Attacks Fall in First Quarter" Accessed May 8, 2018. https://gulfnews.com/business/sectors/technology/ddos-attacks-fall-in-first-quarter-cyber-security-firm-says-1.2032868

[21] Gulf Business. "Weekend slows down WannaCry attacks in the UAE Accessed May 8, 2018. https://gulfnews.com/business/sectors/technology/weekend-break-slows-wannacry-attacks-in-uae-1.2027212

[22] https://www.cia.gov/library/publications/the-world-factbook/fields/2177.html

[23] Symantec."2016 Norton Cyber Security Insights: The UAE" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-comparisons-uae-en.pdf.

[24] Symantec."2017 Norton Cyber Security Insights: The UAE" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-uae-en.pdf

[25] The Arabian Business. "Over 3 million UAE consumers lost 1bn to cybercrime in 2017" Accessed May 8, 2018. http://www.arabianbusiness.com/technology/388166-over-3m-uae-consumers-lost-1bn-to-cybercrime-in-2017

[26] Symantec."2017 Norton Cyber Security Insights: The UAE" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-uae-en.pdf

Phishing is one of the most significant methods of attack in the GCC region, including in the UAE. According to a 2016 Symantec report, the UAE ranked 10th in the world in terms of proportion of email traffic identified as phishing and 7th for proportion of email traffic identified as malicious.[27] Increased malicious code activity in a region or country is often a direct consequence of rapid digitization, specifically "increased broadband penetration and increased competition in the marketplace that can drive down prices, increasing adoption rates."[28] A similarly dangerous combination of factors contribute to the prevalence of phishing and online scams: 1) wide use of digital technologies and services including smartphones, online banking and email 2) lack of cyber hygiene and consumers' unfounded confidence in their ability to protect themselves online. For instance, according to a survey by Dubizzle — the UAE's largest classifieds website— 36 percent of respondents had never heard of the term "phishing" and 16 percent were aware of the term but did not know what it meant.[29] These survey results explain why Dubizzle is a lucrative platform for phishing scammers with 30.8 percent suspected scams on Dubizzle Jobs and 27.6 percent on Dubizzle Motors.[30]

A 2017 report on cybersecurity habits of consumers in the UAE further show common trends that leave users vulnerable. According to Symantec's Cybersecurity Insights report 45 percent of cybercrime victims in the UAE shared the password for at least one account with another person and 20 percent of them use the same password across multiple accounts.[31] As such, cybercrime has seeped into a variety of platforms across the digital sphere including online dating. According to data by the Kaspersky labs, more than half of online dating users have experienced a cyber threat or problem. The trend of inadequate cyber hygiene continues in online dating users as well: 25 percent of users in the UAE share their full names publicly on online dating profiles while 15 percent share their home addresses and 9 percent share photos of family members.[32]

c) **State of national cybersecurity strategy**

Cybersecurity has been on the forefront of the UAE's policy making and defense strategy since the country's financial institutions and government agencies were hit by cyber attacks in 2012, 2013 and 2014[33]. As part of a new push for cybersecurity defense, the UAE was set to double its spending on homeland security to more than $10 billion by 2024 with a majority of the funding

[27] Symantec. "Government Internet Security Report" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-government-en.pdf.
[28] Ibid.
[29] https://fraudwatchinternational.com/phishing/uae-gcc-region-importance-increasing-phishing-awareness/
[30] The Arabian Business. "One Third of Cyber Scam Victims Failed to Take Action" Accessed May 8, 2018. http://www.arabianbusiness.com/one-third-of-cyber-scam-victims-failed-take-action--673122.html
[31] Symantec."2017 Norton Cyber Security Insights: The UAE" Accessed May 8, 2018. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-uae-en.pdf
[32] "50% of Online Dating Users in UAE Experienced IT Security Incidents." *Dubai Eye* (blog), February 14, 2018. http://dubaieye1038.com/50-of-online-dating-users-in-uae-experienced-it-security-incidents/.
[33]

aimed at strengthening cybersecurity.[34] However many experts suggest that despite progress and increased investment the country's cyber defenses are inadequate.[35] In addition to the country's reliance on Internet of Things and an increasingly connected society, the larger framework of Middle Eastern politics and conflicts mean that the UAE is a valuable target for state generated intelligence gathering efforts. In this regard, Iranian and Israeli cyber attack capabilities pose significant threats to the UAE.[36]

In terms of tactical defense, the UAE has doubled down on cybersecurity spending including plans to form a cyber command within the General Headquarters (GHQ) of the UAE Armed Forces.[37] Furthermore, the UAE uses malware to defend against terrorists and cyber criminals. Most recently this practice came under scrutiny after it was revealed that the Emirati government bought a zero-day Israeli exploit for Apple's iOS to allegedly surveille a domestic dissident.[38]

In addition to the military and technical defense, the UAE's most significant step in ensuring cybersecurity preparedness came in 2014 when the National Electronic Security Authority (NESA) published the Emirates' national cyber strategy.[39] The national strategy also outlines standards and policies including Critical Information Infrastructure Policy (CIIP), and the UAE Information Assurance (IA).[40] NESA's mandates include: 1) defend and respond, 2) protect critical infrastructure, 3) improve threat awareness, 4) develop human capital, 4) develop technical abilities, 5) cooperate with partners. Furthermore, The UAE has an officially recognized national cyber incident report team (CIRT) known as aeCERT.[41] This well-articulated national cyber strategy and clearly-defined goals put the UAE ahead of many other states in terms of cyber preparedness.

---

[34] "UAE To Double Security Budget, Focus on Cyber." *Military Edge: The Most Comprehensive Tool on the Web for QME* (blog), February 24, 2014. https://militaryedge.org/articles/uae-double-security-budget-focus-cyber/.
[35] The Arab Gulf States Institute in Washington. "Bridging the Cybersecurity Talent Gap." Accessed May 8, 2018. http://www.agsiw.org/wp-content/uploads/2016/02/Cybersecurity-Forum-Report.pdf.
[36] Lewis, James Andrew. "Cybersecurity and Stability in the Gulf" Center for Strategic & International Studies. Accessed May 8, 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf.
[37] "UAE Military To Set Up Cyber Command." Accessed May 8, 2018. http://www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command.
[38] Groll, Elias. "The UAE Spends Big on Israeli Spyware to Listen In on a Dissident." Foreign Policy *(magazine)* Accessed May 8, 2018. http://foreignpolicy.com/2016/08/25/the-uae-spends-big-on-israeli-spyware-to-listen-in-on-a-dissident/.
[39] Lewis, James Andrew. "Cybersecurity and Stability in the Gulf" Center for Strategic & International Studies. Accessed May 8, 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140106_Lewis_GulfCybersecurity_Web_0.pdf.
[40] The Arab Gulf States Institute in Washington. "Bridging the Cybersecurity Talent Gap." Accessed May 8, 2018. http://www.agsiw.org/wp-content/uploads/2016/02/Cybersecurity-Forum-Report.pdf.
[41] Ibid.

As part of the global growing cybersecurity workforce gap, the UAE also needs more qualified cybersecurity workers to join its workforce both in private and public sectors. In addition to online safety workshops aimed at young people and children, the government has undertaken longer-term projects such as the establishment of Information Security Research Center (ISRC) at the Khalifa University, which offers the country's only MSc and PhD degreees in cybersecurity.[42]

The UAE owes much of its digital leader status in the region to the government's push for innovation and technology use. Dubai is often put in the center of such efforts. In addition to the national strategy, Prime Minister of the UAE and Rules of Dubai Sheikh Mohammed bin Rashid Al Maktoum launched the Dubai Cybersecurity Strategy in 2017 to strengthen the financial capital's defenses and global perception.[43] Similarly, Sheikh Mohammed launched the "Data Wealth" initiative which aims to protect Dubai's government and consumer data. The multipronged innovation strategy also includes furthering Internet of Things (IoT) penetration and turning Dubai into a "smart city."[44] While this strategy on its own isn't worrisome on its own, researchers warn that about the security of IoT systems. As such, use and adoption of IoT technologies in Dubai — as well as the rest of the UAE — raises security concerns among experts.[45]

4. Action Items, Lessons and Recommendations

Connectivity brings vulnerability

As the United Arab Emirates pushes for more digitization and innovative uses of technology in areas of life including in e-government, Internet of Things and online banking, it must be ready to take on an equally heavier load of cyber attacks. The significant use of such technologies and the increasingly connected population provide alluring targets for cybercriminals and makes the UAE into a lucrative target. In the rapidly evolving landscape of cyber attacks, enhanced connectivity means heightened vulnerability and the sophistication of cyber attacks put both organizations and individuals at risk. Therefore, the UAE should double down on its efforts to implement security wide standards and policies at the same rate it invests in new technologies.

---

[42] Ibid.
[43] Emirates 24 News. "Sheikh Mohammed Launches Dubai Cyber Security Strategy." Accessed May 8, 2018. https://www.emirates247.com/news/emirates/sheikh-mohammed-launches-dubai-cyber-security-strategy-2017-05-31-1.653840

[44] Arabian Business. "Dubai Launches Strategy to Build Smart City" Accessed May 8, 2018. http://www.arabianbusiness.com/industries/technology/381782-dubai-launches-strategy-to-build-worlds-most-advanced-iot-ecosystems
[45] Bodhani, Aasha. "UAE security analysts find vulnerabilities in IoT devices" Accessed May 8, 2018. http://www.itp.net/607209-uae-security-analysts-find-vulnerabilities-in-iot-devices

Misplaced trust in security online and the importance of cyber hygiene

As evidenced by high numbers of individuals experiencing cybercrime in 2017 as well as 2016, the UAE digital consumer has a hygiene problem. Dangerous user habits and attitudes — like using the same password across multiple accounts and sharing passwords with third parties — revealed themselves in consumer surveys. Furthermore, lack of hygiene is coupled with a growing young population and increased familiarity with technology across generations to create a dangerous combination. The UAE should not treat cybersecurity as an IT issue and invest in increasing user awareness of basic cyber hygiene through educational campaign. Educating the consumers — particularly the tech-savvy young demographic — would help strengthen the weakest link in cybersecurity: humans.

Putting the strategy into action:

The recent push for further digital penetration and innovation is a clear sign that in the scale of risk and opportunity, the UAE is investing in digitization for financial and political gains. The accompanying security measures including and especially the newly articulated National Cybersecurity Strategy are all steps in the right direction. However to fully minimize cyber risk and reap benefits of a digital economy the next step is to move forward from initial focus areas to realizing concrete goals and objectives. Building a cybersecurity workforce by investing in cybersecurity capacity building and training and focusing on the intersection of digital economy and security are beneficial implementations of the strategy.

5. Conclusion

As a regional leader of digitization and a global financial, cultural hub, the United Arab Emirates is in the unenviable position of having to defend against a continuous stream of cyber attacks and lead the region toward cybersecurity preparedness. The tech-savvy young population, heightened connectivity levels and technology penetration rates mean that the Emirates is vulnerable to attacks from many sides including financially motivated cybercriminals and regional political rivals. Despite increased investment in cybersecurity preparedness — including workforce building efforts and the dissemination of a national cybersecurity strategy — more than half of the UAE population experience cybercrime in 2017 and more than 3 billion dollars were lost. In order for the UAE to reach its maximum digital potential and fully reap the benefits of innovation, security must be on the forefronts of policy making and investment for the foreseeable future. In particular, focus must be on emerging technologies like Internet of Things which are not only prevalent in the UAE but have known security vulnerabilities open to exploitation. Furthermore, transparency in incident sharing and regional cooperation are areas where the UAE's cybersecurity strategy can be improved for full efficiency in defending against and combating cyber threats.