<table>
<thead>
<tr>
<th>TABLE OF CONTENT</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>01 EXECUTIVE SUMMARY</td>
<td>5</td>
</tr>
<tr>
<td>02 SECURING THE SMART CITY</td>
<td>7</td>
</tr>
<tr>
<td>03 EXPANDING RISKS</td>
<td>15</td>
</tr>
<tr>
<td>04 THREAT LANDSCAPE</td>
<td>20</td>
</tr>
<tr>
<td>05 SELECTED GLOBAL SECURITY INCIDENTS</td>
<td>25</td>
</tr>
<tr>
<td>06 CASE STUDY: EXPO 2020 DUBAI</td>
<td>27</td>
</tr>
<tr>
<td>07 CURRENT UAE ATTACK SURFACE</td>
<td>29</td>
</tr>
<tr>
<td>08 SUMMARY</td>
<td>31</td>
</tr>
<tr>
<td>09 ACTIONABLE TAKEAWAYS</td>
<td>32</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

01.

Smart Cities are expected to unlock enormous efficiency and productivity gains for the UAE and other nations. However, the Internet of Things (IoT), the technology underpinning these complex and interconnected urban networks, offers a considerably expanded attack surface for cyber adversaries of all kind.

Digital14’s first Cyber Resilience Report for 2020 is published as public and private sector organisations begin to focus on the multidimensional impact of the IoT. This document delineates the exponential growth of the threat landscape and outlines the technologies being targeted in the UAE as the nation implements Smart City projects in 2020 and beyond. Finally, the report also offers trustworthy, actionable recommendations for leaders and decision-makers.

The UAE ranks first in the Middle East and 23rd of 79 countries in the world in the Global Connectivity Index (GCI), which measures countries’ progress on digital transformation. Accordingly, Smart City projects are underway across several emirates, encompassing a variety of sectors. The lifeblood of these developments is a common technology: the IoT. By 2022, Cisco expects 51% of all networked devices to be IoT-enabled, bridging the gap between the physical and virtual worlds in dynamic new ways. For UAE residents, Smart Cities will bring an improved quality of life, more efficient and sustainable governance, and productive new business solutions.

The highly networked environment that UAE companies operate within provides rich pickings for cybercriminals, offering easy opportunities to release prolific malware that can cause catastrophic and often life-threatening damage in the real world, or stimulate lucrative criminal enterprises.

On the other hand, the global research and advisory firm Gartner reports that 20% of organisations around the world have faced at least one IoT attack and in 2020, a quarter of all attacks that organisations face will be IoT-based. These attacks will occur with increasing frequency. The UAE clocked an average of 304 IoT-based attacks on a daily basis in 2019.

The UAE’s aim in adopting Smart City initiatives is to improve virtually all sectors of urban living. However, the technologies used for this purpose are already under attack from both cybercriminals and nation-states, further raising future security risks for this advanced Arab economy. With the upcoming Expo 2020 Dubai poised to serve as the prototype for the region’s first Smart Cities, organisations within the country and the region must act now to secure every aspect of their business – and remain vigilant as the attack surface expands exponentially.

There were 22 billion networked devices worldwide, according to one estimate; by 2025, that number will rise to 38.6 billion. Each of these devices serves as an entry point for cybercriminals. IP cameras and digital video recorders (DVRs) can be manipulated to bring down networks in Smart Healthcare and Smart Mobility sectors, while industrial control systems can be exploited to disable large parts of the Industrial Internet of Things (IIoT) in sectors such as Smart Buildings, Smart Energy and Smart Infrastructure.

Data breaches remain another critical area, where personal records are often easily stolen without sophisticated or expensive equipment. By 2025, networked devices will generate over 79.4 zettabytes of data every year, a significant portion of it for Smart City initiatives. At present, 91.5% of IoT transactions are sent over the Internet in plain text, via unsecured communications channels that serve up this confidential information on a platter.

The highly networked environment that UAE companies operate within provides rich pickings for cybercriminals, offering easy opportunities to release prolific malware that can cause catastrophic and often life-threatening damage in the real world, or stimulate lucrative criminal enterprises.

May 2020

Cyber Resilience Report
SECURING THE SMART CITY

A. What is a Smart City?

There are several ways to define a Smart City, but all the definitions hold one principle at their core: using technology to solve the long-term challenges produced by increasing urbanisation. Depleting resources, greater demands on limited infrastructure and other environmental issues must be tackled in order to enhance the city’s liveability, workability and sustainability. Smart Cities, then, are connected, responsive, and intelligent.

The vast majority of UAE residents – about 87% of the population – lived in urban areas as of 2018, and the figure is set to grow to 92% by the year 2050. But with fewer resources available to an expanded population, the country’s urban systems will need to perform much more efficiently to deliver the same level of services their residents enjoy today. In line with its reputation for visionary thinking, the UAE government has therefore launched a range of e-government initiatives that harness a wide array of digital technologies in the creation of Smart Cities.

Digital14 outlines what such a Smart City could look like (see Figure 1), based on the report, The Vision of a Smart City, presented at the 2nd International Life Extension Technology Workshop in Paris on September 28, 2000:

A city is Smart when investments in human and social capital, traditional infrastructure, and disruptive technologies fuel sustainable economic growth and a high quality of life, coupled with prudent management of natural resources through participatory governance. In Smart Cities, Information and Communication Technology (ICT) is seamlessly integrated into the city’s infrastructure and is imperceptible to its end users.
B. The smart city value chain: better connected but more exposed

A Smart City initiative may be vulnerable to security risks in several ways across its value chain (see Figure 2). The different possible attack points range across a four-layer architecture: devices, transmission, the Smart City platform itself, and various sector-specific applications. Security risks surface mainly from the three underlying layers, but a hazard arising from any layer may affect numerous applications. In this regard, every layer of the Smart City’s value chain must be secured.

C. Security risks in smart sectors

Smart Cities encompass a number of initiatives designed to improve services provided to individuals and organisations within the environment. Digital14's research focused on security risks in the following eight sectors:

- **Smart Governance**: The primary objectives of Smart Building initiatives include improving the efficiency and reducing consumption and energy costs. By their very nature, Smart Buildings must be accessible to a range of different stakeholders. They are therefore hosted on publicly accessible websites, which puts their security at stake. Security vulnerabilities at such public-facing systems include interfaces that either require no authentication at all or use default credentials.

- **Smart Buildings**: Initiatives for Smart Citizens aim to maintain active learning and establish a feedback loop of innovative ideas for the continued development of the Smart City. Through residents' voluntary contribution of personal data, authorities are empowered to make better decisions. The confidential nature of this data necessitates the proper upkeep of its collection and storage. Any breaches or misuse of information could dissuade future citizen participation and derail further development.

- **Smart Citizens**: Smart energy initiatives are deployed to achieve a cost-effective, environment-friendly, and sustainable use of energy. Sensors are widely deployed to monitor and manage energy across the cycle from generation to consumption. The security of Smart Grids is paramount since its disruption or failure has the potential for devastating consequences. Complex viruses could be deployed against Smart Grids to steal sensitive data, gain unauthorised system control, disrupt power supplies, or even cause physical damage.
Digitisation of government data increases cybercriminals’ motivation for successful hacks and steal data. Example Attack | Records of 1.5 million patients of Singapore Health Services (SingHealth) were accessed and stolen by sophisticated threat actors.

The centralised device management of smart devices, being a “one-stop-shop,” is a lucrative target for cybercriminals to wreak havoc. Example Attack | Kaspersky researchers hack colleague’s smart Fibaro Home Center 2.

Devices supporting automation for large metropolitan areas provide cybercriminals an avenue to cause widespread chaos and physical damage. Example Attack | Stuxnet worm targeted Siemens S7 PLC as part of the campaign to sabotage Iranian centrifuges.

If Smart Infrastructure is the backbone of a Smart City economy, then Smart Technology is its beating heart and likewise transcends various sectors in the modern city ecosystem. However, the road to security maturity for most IoT devices remains considerably lengthy. An IBM overview of 17 zero-day vulnerabilities affecting popular IoT devices such as default credentials or SQL injections shows that many vendors have yet to reach the required level of maturity and are preoccupied with capability over security.26

Figure 3. General threats and actual attacks in smart city sectors.
D. The UAE’s smart city initiatives

From being an early adopter of e-government initiatives to offering smart services for citizens and residents on mobile devices, the UAE has leveraged a number of new technologies to create a Smart Nation with applications that match or transcend global standards. Since each smart sector adopts technologies to enable its own specific goals, application levels vary across all sectors, and some solutions are more actively exploited than others.

The UAE’s digital transformation is spearheaded by Abu Dhabi and Dubai, with initial Smart City projects launched by Fujairah and Sharjah. The UAE leads the Middle East and ranks 23rd of 79 countries in the world on the 2018 Global Connectivity Index (GCI), a global measure of digital transformation. There are two principal Smart City projects in the UAE. Smart Abu Dhabi provides operational support for the ICT integration of the emirate’s government, and the management of its agencies’ institutional and development functions. Smart Dubai 2021 uses happiness as the ultimate success indicator. Figure 4 provides examples of key UAE Smart City projects from October 2018 to October 2019. The presence of initiatives in all the eight sectors highlights the UAE’s continuing commitment towards digital transformation, underscoring its high rank on global indices.

E. The lifeblood of the smart city: the IoT

Smart Cities around the world, including in the UAE, rely on a range of technologies from smart grids to global positioning systems. In turn, all these are underpinned by the Internet of Things (IoT), a revolutionary communications model comprised of an invisible, innovative framework that connects digital devices to the internet. Sensors within such IoT-enabled devices communicate, collect, and exchange data with other devices across the value chain. This data is then analysed to optimise products, services and businesses with the end goal of improving the quality of life for a Smart City’s inhabitants.

With an increasing number of countries seeking to unlock the benefits of Smart Cities, the IoT market is recording double-digit growth. International Data Corporation (IDC), the market intelligence firm, forecasts that the worldwide IoT market will reach $1.2 trillion by 2022, a compound annual growth rate (CAGR) of 13.6% between 2017-2022. Cellular IoT connections alone are expected to reach $3.5 billion in 2023, clocking a CAGR of 30%.

Those projections represent billions of devices, any one of which may be compromised if improperly secured. Given this exponential growth, securing the IoT and Smart Cities in general becomes critically important. The UAE’s technology-driven Smart City initiatives rely on reliable and trusted IoT-connected supply chains to enhance efficiencies for businesses and residents, but those new systems bring new types of security risks.
As we have seen, the very networks that support Smart Cities open them up to unprecedented levels of risk. With the number of networked devices growing to tens of billions, those risks will expand exponentially across a broader attack surface. According to Cisco’s Visual Networking Index, IoT connections will grow to 51% of networked devices worldwide by 2022. Digital14 examines how those risks can play out:

Vulnerabilities are now being seen in devices in sectors such as the Smart Healthcare and Smart Mobility. In Smart Healthcare, for example, vulnerabilities have been found in pacemakers and insulin pumps. By exploiting those weaknesses, malicious actors could launch untraceable, severe attacks across the entire system. In the Smart Mobility sector, a 2014 study highlighted weaknesses in the traffic infrastructure of a Michigan road agency; attackers were able to control over a hundred traffic lights after compromising the system. Multiple vulnerabilities have also been discovered in Tesla vehicles, one of which allowed attackers to remotely activate the braking mechanism. As more semi-autonomous vehicles make it onto city streets, such vulnerabilities will become more common.

Smart City technologies also extend to the industrial world and its subset of the IoT, the Industrial Internet of Things (IIoT). While most observed cyberattacks have not as yet led to catastrophic physical disruptions, the intent and ability to cause life-threatening physical consequences is evident, as seen in past cyberattacks against industrial control systems (ICS). The Stuxnet malware that targeted Iranian centrifuges, first revealed publicly in 2010, was specifically intended to disrupt an industrial process.

Assessing the number of networked devices in use worldwide is challenging because of the nature of collating such estimates. What remains indisputable, is that the number of connected devices will rise as IoT expands its reach. Strategy Analytics appraised the number of networked devices at 22 billion as of the end of 2018, a number forecast to rise to 38.6 billion devices by 2025.

Each IoT device hosts technologies that any persistent threat actor may target to access an organisation’s network. And IoT devices are being constantly hit to gain initial entry. Gartner reports that 20% of organisations observed at least one IoT-based attack from 2015 to 2018. By 2020, more than 25% of attacks against enterprises will involve IoT devices. Yet, a 2018 survey of 950 companies that make and use IoT technology found that just under half - 46% - do not have detection mechanisms in place to protect against cyber attacks. About 79% of respondents believed governments should lead efforts to set and enforce tougher IoT security standards.

The IoT’s growing use presents an attractive target for botnet operators seeking to boost the capabilities of their malware for malicious tasks such as distributed denial of service (DDoS) attacks. In October 2016, US-based web application security company Dyn confirmed being targeted by malicious attack traffic. The company confirmed that the Mirai botnet as the primary source, with the involvement of nearly 100,000 malicious end points. The attack brought down websites, mostly based in the US and Europe, such as Twitter, the Guardian, Netflix, Reddit, CNN and many others. The botnet achieved this with the help of approximately 145,000 IoT devices, principally IP cameras and DVRs. Assessing the number of networked devices in use worldwide is challenging because of the nature of collating such estimates. What remains indisputable, is that the number of connected devices will rise as IoT expands its reach. Strategy Analytics appraised the number of networked devices at 22 billion as of the end of 2018, a number forecast to rise to 38.6 billion devices by 2025. The IoT’s growing use presents an attractive target for botnet operators seeking to boost the capabilities of their malware for malicious tasks such as distributed denial of service (DDoS) attacks. In October 2016, US-based web application security company Dyn confirmed being targeted by malicious attack traffic. The company confirmed that the Mirai botnet as the primary source, with the involvement of nearly 100,000 malicious end points. The attack brought down websites, mostly based in the US and Europe, such as Twitter, the Guardian, Netflix, Reddit, CNN and many others. The botnet achieved this with the help of approximately 145,000 IoT devices, principally IP cameras and DVRs. As more devices are networked, we expect the threat capabilities of such botnet and the potential pool of target devices, to expand correspondingly.

Furthermore, onboarding the technology and devices required to support Smart City initiatives also presents adversarial nation-states with a target-rich environment for both espionage (by gathering data on all niches of a city’s pattern of life), and/or sabotage (by crippling a Smart City’s infrastructure).
ICS has been subjected to persistent attacks for at least a decade as threat actors have successfully targeted industrial processes over this period. The IIoT, while further improving the connectivity of ICS-managed infrastructure, could expand the existing attack surface of ICS-managed infrastructure. Networked controls in Smart Buildings could offer one access route, for example. Many of the technologies being used to develop sectors such as Smart Energy, Smart Infrastructure, and Smart Buildings will build on pre-existing functionalities that have enabled automated manufacturing and industrial controls for decades. While IIoT disruptions are significantly fewer than the number of global cyberattacks, past ICS attacks demonstrate the presence and intent of such disruptions. Accordingly, cities will have to defend against them as smart initiatives progress.

Through unprotected IIoT networks, threat actors will be able to develop malware, techniques, tactics and procedures that can be aimed at different, geographically diverse organisations. The majority of active threats targeting the IoT are borne by self-propagating malware or cyberespionage vectors, yet modernised industrial processes will allow threat actors a new set of opportunities to carry out physical disruptions with severe consequences. Without controls such as network security monitoring, anomalous activity detection and accurate network device discovery, industrial sites are at an increased risk of attack.

A May 2019 report by information security company Zscaler examined approximately 56 million IoT transactions processed over a 30-day period. Approximately 91.5% of these were communicated without proper encryption. The transactions were made from 270 different types of IoT devices made by 153 different manufacturers. Separately, a November 2019 report from CyberX analysed 1,821 IoT/ICS networks over the previous year. About 64% had unencrypted or clear text passwords across their networks, and 54% of the networks could be accessed remotely using standard protocols such as remote desktop protocol (RDP), secure shell (SSH), and virtual network computing (VNC).

Much of the value of Smart City technologies lies in the lucrative data they generate, from the granular details of road traffic movements to databases of personally identifiable information (PII). According to IDC estimates, global devices will generate over 79.4 zettabytes of data collectively in 2025. Cybercriminals and nation-state actors value this information, particularly data concerning PII, intellectual property, and the socio-economic environment of another country’s population.

As we have seen in the United States, the theft of personal records through data breaches has mounted steadily over the past decade. Such data breaches do not always require sophisticated attacks or significant resources. Since any data generated or used by the Smart City must be stored, cybercriminals need merely to scout for improperly secured data repositories. Database administrators often fall short of basic security precautions such as strong authentication credentials or segmenting such databases from public exposure.

Safeguarding data in transit presents another major challenge for projects integrating IoT solutions. Digital14 has identified several pain points regarding secure data transmission in Smart City projects:

- Deploying and scaling low-energy secure protocols and encryption schemes on networks and devices
- Enforcing safe and secure communication while bridging the cyber-physical security gap, and,
- Safeguarding privacy and enforcing data anonymity whenever applicable.

A May 2019 report by information security company Zscaler examined approximately 56 million IoT transactions processed over a 30-day period. Approximately 91.5% of these were communicated without proper encryption. The transactions were made from 270 different types of IoT devices made by 153 different manufacturers. Separately, a November 2019 report from CyberX analysed 1,821 IoT/ICS networks over the previous year. About 64% had unencrypted or clear text passwords across their networks, and 54% of the networks could be accessed remotely using standard protocols such as remote desktop protocol (RDP), secure shell (SSH), and virtual network computing (VNC).
A. Targeted technologies

IoT technologies, whether currently in use or soon to be deployed, will continue to face persistent threats. The Mirai family of botnets, in particular, targets devices commonly used at home, such as routers, DVRs, and IP cameras. This malware family aims specifically at IP cameras and routers, which link together all the networked devices in a home or workplace. These items are under constant threat of detection by botnets, which continuously scan public-facing devices over the internet.

IoT devices in healthcare and transportation sectors have also been compromised in the past. In June 2019, NewSky Security researchers observed ongoing attacks against a web-based DNA sequencer, where attackers exploited a vulnerability within the application and gained access to the underlying systems. In November 2016, a DDoS attack targeting two buildings in Finland disabled the sensors monitoring data such as temperature and radiator pressure, in the process also disabling the safety mechanism to shut down systems.

In 2018 and 2019, xentLabs researchers discovered four vulnerabilities in popular lines of Sony Smart TVs. After notifying Sony and providing them with a reasonable time to fix the vulnerabilities, this information was later disclosed publicly. One weakness affects the Photo Sharing Plus app installed on numerous TV models. By leveraging the Photo Sharing Plus API, an unauthenticated remote attacker could retrieve the Wi-Fi credentials of the home or office where the Smart TV was being used. Such information could provide an attacker with a powerful pivot into a corporate network. The other vulnerability allows an unauthenticated attacker to read arbitrary files on the device. These weaknesses reflect the risks inherent in increased connectivity across everyday activities.

Smart Cities are designed to increase productivity and efficiency for everyone, but they could present potentially serious risks when cybersecurity is neglected. The spread of IoT devices exposes a wide range of vulnerabilities that cybercriminals and other malicious actors can exploit for various purposes.
B. Threats

Cybercriminals with differing levels of expertise are actively looking for – and finding – ways to penetrate into IoT devices. The system’s exponential adoption coupled with improper safety precautions offers them innumerable routes to successful infiltration.

Active threats against the IoT are already present, but self-propagating malware dominates the landscape in terms of volumes of attack and effect. High-profile malware, such as the Mirai variants, have wreaked havoc on both traditional network resources and IoT devices. Critically vulnerable IoT devices are widely deployed across homes, businesses, and municipal environments, constituting a particularly attractive canvas for botnets to spread.

A Kaspersky report released in October 2019 revealed Mirai and its variants as the top threats against IoT devices in the first half of 2019. Over the same period, Kaspersky identified Linux. NyaDrop.b as the most prolific Mirai variant.

Mirai and its derivatives remain the most common IoT malware. First discovered in August 2016, Mirai quickly spread to routers, DVRs and IP cameras by leveraging vendor-supplied default credentials. The botnet was responsible for significant DDoS attacks that year. By October 2016, Mirai’s author had published its source code, allowing it to be repurposed into several Mirai malware variants (see Figure 6). These new versions have been deployed in a number of different exploits to countless new devices. The variant Echobot, for instance, targets both IoT and non-IoT technologies such as application servers and networking software.

Malware is often a commercial commodity available for purchase by both cybercriminals and nation-state actors. Thus, the authors of a particular software may not be the ones actually using it to trigger attacks. In the case of TheMoon botnet, vulnerable routers and modems were targeted in order to expand its botnet infrastructure. By 2019, updates to the botnet’s malware had transitioned into a commercial service. TheMoon has been designed for commercial purposes and can be leased to any threat actor willing to pay. Its attacks on the IoT are often aimed at expanding its commercial applications.

The origin of prolific IoT malware goes back to 2009, when the self-propagating PsyB0t compromised tens of thousands of routers running MIPSel Linux firmware by exploiting weak default credentials. Besides Mirai, more distinct malware families have emerged (see Figure 7), with most exploiting authentication issues to gain initial access to vulnerable IoT devices.
While the distinctions between cybercriminals and nation-state groups behind cybersecurity threats have long been muddied by difficulties in attribution, threat actors specific to IoT operate within an even more nebulous environment. The main difficulty in defining threat actors arises because malware designed to create botnet-as-a-service applications overshadows specifically targeted breaches.

In 2018, malware and botnets comprised the vast majority of threats and successful attacks against the IoT. Such threats are rarely linked to specific actors. However, specific malicious actors such as the Russian cyber-espionage group, APT28 (also called Strontium, Sofacy Group, or Fancy Bear), have targeted multiple organisations by first aiming at office printers, video decoders and voice-over-IP (VoIP) phones. Here, the attacked IoT devices were not the primary targets but functioned as launch pads to achieve greater destruction within the recipients’ networks.

Other threat actors have been pinned to specific attacks, even if any agenda or associations to specific countries or groups are unknown. For example, Slingshot, named after malware observed by Symantec in 2018, compromised routers to deploy handcrafted espionage tools. Although the botnet-as-a-service model conceals culprits behind most IoT botnet activities, a black hat hacking group known as Lizard Squad has been connected to at least one botnet, known as LizardStresser.

<table>
<thead>
<tr>
<th>APT28</th>
<th>Motivation</th>
<th>Espionage</th>
<th>Targeted IoT Devices</th>
<th>Routers, NAS, VoIP phones, office printers, video decoders</th>
<th>Malicious Tool</th>
<th>VPN filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last reported date: 2018 May 24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slingshot</th>
<th>Motivation</th>
<th>Unknown</th>
<th>Targeted IoT Device</th>
<th>Routers</th>
<th>Malicious Tools</th>
<th>Cahnadr (aka Ndriver), GoliuApp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last reported date: 2018 March 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lizard Squad</th>
<th>Motivation</th>
<th>Unknown</th>
<th>Targeted IoT Devices</th>
<th>WiFi-enabled cameras and surveillance systems</th>
<th>Malicious Tool</th>
<th>LizardStresser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last reported date: 2016 September 29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sophistication</th>
<th>Target Country</th>
<th>Nation-State</th>
<th>Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Country</td>
<td>Target Countries</td>
<td>UAE, Yemen, Jordan, Turkey, Iraq, Libya, Afghanistan, Kenya, Congo, Sudan, Somalia, Tanzania</td>
<td></td>
</tr>
<tr>
<td>Sophistication</td>
<td>Target Countries</td>
<td>Unknown</td>
<td>USA, Brazil</td>
</tr>
</tbody>
</table>
SELECTED GLOBAL SECURITY INCIDENTS

Los Angeles, California
21 Aug 2006
Two traffic engineers hacked into the city’s Traffic Surveillance Center and disabled the signals, causing gridlock for several days

Rye Brook, New York
28 Aug – 18 Sep 2013
Iranian hackers breached computer-guided controls of Bowman Avenue Dam accessing status and operation data

Estonia
27 Apr – 18 May 2007
Pro-Russian hackers launched DDoS attacks on Estonia’s key government websites rendering them inaccessible for days

Germany
2014
Unknown attackers used spear phishing mail to access a steel works facility resulting to unscheduled closure of the furnace

Ukraine
23 Dec 2015
BlackEnergy malware planted in networks of multiple power companies in Ukraine, and led to blackouts in different regions

Lappeenranta, Finland
Nov 2016
Cybercriminals launched DDoS attack on the building management systems knocking out heating controllers

Dallas, Texas
6 Apr 2017
Hackers activated the emergency outdoor sirens with a rogue radio signal causing misinformation and panic among residents

New Delhi, India
9 Apr 2017
Three civilians exploited an accessible Wi-Fi port at a metro station in New Delhi and played a pornographic clip causing disruption

Sweden
11 – 12 Oct 2017
Suspected nation state group launched DDoS attack on Sweden’s transportation system causing train delays

Bristol, United Kingdom
14 Sep 2018
Unknown attackers launched ransomware attack at Bristol Airport causing a shutdown on flight display screens

Figure 8. Global Security Incidents in Smart Cities.69

Los Angeles, California
21 Aug 2006
Two traffic engineers hacked into the city’s Traffic Surveillance Center and disabled the signals, causing gridlock for several days

Rye Brook, New York
28 Aug – 18 Sep 2013
Iranian hackers breached computer-guided controls of Bowman Avenue Dam accessing status and operation data

Estonia
27 Apr – 18 May 2007
Pro-Russian hackers launched DDoS attacks on Estonia’s key government websites rendering them inaccessible for days

Germany
2014
Unknown attackers used spear phishing mail to access a steel works facility resulting to unscheduled closure of the furnace

Ukraine
23 Dec 2015
BlackEnergy malware planted in networks of multiple power companies in Ukraine, and led to blackouts in different regions

Lappeenranta, Finland
Nov 2016
Cybercriminals launched DDoS attack on the building management systems knocking out heating controllers

Dallas, Texas
6 Apr 2017
Hackers activated the emergency outdoor sirens with a rogue radio signal causing misinformation and panic among residents

New Delhi, India
9 Apr 2017
Three civilians exploited an accessible Wi-Fi port at a metro station in New Delhi and played a pornographic clip causing disruption

Sweden
11 – 12 Oct 2017
Suspected nation state group launched DDoS attack on Sweden’s transportation system causing train delays

Bristol, United Kingdom
14 Sep 2018
Unknown attackers launched ransomware attack at Bristol Airport causing a shutdown on flight display screens

Figure 8. Global Security Incidents in Smart Cities.69
Background
One of the most anticipated World Expos of all time and the first ever to be hosted in the Middle East, Africa and South Asia (MEASA) region, Expo 2020 Dubai will host millions of visitors from across the world throughout its six-month run. With such a large number of visitors expected throughout the duration of Expo, as well as the fact that up to 130 buildings across the 4.38-square-kilometer site will be interconnected via Internet of Things (IoT), there is a cyber security risk to the event’s infrastructure and operations. Therefore, all associated challenges relating to IoT security must be addressed. The digital infrastructure of Expo 2020 crosses several smart city domains and sub-domains, and a breach of IoT security and subsequent cyber-attack could pose a risk to the infrastructure and operational capacities of the event and ultimately damage its reputation.

The challenge
Expo 2020 will be one of the largest World Expos to date. More importantly, however, Expo 2020 Dubai is expected to be one of the most digitally advanced World Expos ever held. IoT connectivity represents a critical component of the event’s digital infrastructure, and the latest IoT technologies will be used across the entire IoT infrastructure and Expo 2020 site. Without appropriate cyber security protocols, IoT applications would be vulnerable to cyber attacks. The visibility of this physically connected infrastructure also poses a further risk given a breach could be observed by millions of visitors. A robust Security Operation Center (SOC) is critical to ensuring a seamless event and avoiding any incidents that may impact infrastructure and operations. The IoT ecosystem is particularly sensitive, emphasizing the need for enhanced data privacy and protection. The overarching goal is to safeguard the visitor experience and ensure the event serves as a proud legacy for Dubai and the UAE.

The digitalized event becomes, the more vulnerable it is to security breaches, which presents a significant cyber security challenge. Because Expo 2020’s digital agenda entails a unique and seamless digital user experience, cyber security is essential for the protection of data, infrastructure, and the network, as well as monitoring all operations. The event’s cyber security operations will revolve around the safety of all international participants and millions of visitors. A major threat is the risk of data leakage, which could have detrimental internal and external consequences. To counter this, Digital14 will create and maintain a solid foundation for a smart city environment and ensure a smooth and secure digital experience. Any event requires cyber security of the highest possible standards due to its critical nature and the extensive cyber-attack surface presented by its digital footprint. To counter such risks, Expo 2020 requires innovative cyber security solutions, ground-breaking initiatives and ongoing services to secure new technologies and support cross-partner flexibility and functionality. On top of this, Expo 2020 aims to strike a balance between local and international best practice and regulations in data privacy and to comply with the General Data Protection Regulation (GDPR) – ensuring the safety and privacy of Expo visitors’ data.

The solution
A homegrown UAE-based organization, Digital14 enjoys the reputation of a reliable and proven cyber security partner. Digital14 has a proven track record of working alongside many government entities across critical infrastructures, delivering an integrated, holistic approach to cyber security while enabling enhanced visibility over all elements of a project.

In the context of a holistic cyber security framework, Digital14 will provide continuous application and infrastructure security monitoring, risk assessment, incident response, and digital forensics to ensure Expo 2020 will be one of the safest and most technologically secure World Expos ever held. At the core of its mandate as Expo 2020 Dubai’s Official Cyber Security Provider, Digital14 will oversee the cyber security of the event’s entire digital platform – as well as the applications and data it supports – to safeguard the digital experience of millions of visitors and more than 190 international participants.

Digital14 is responsible for delivering and managing a next generation Security Operations Center (SOC) for the duration of Expo 2020. This will provide increased visibility across critical areas in Information Technology, Operational Technology, and IoT. At the same time, it will support robust cyber security protocols and a resilient cyber security environment that delivers situational awareness, reduces risk and/or downtime, supports audit and compliance, prevents and controls threats, diminishes administrative overheads, and provides log forensics and reporting.

The team will detect, report, and respond to cyber security incidents throughout the organization to minimize disruption to Expo 2020. Incident priority will be determined according to the impact of the incident on Expo 2020’s business and the urgency of the required response. In case of an incident, the primary concern is to restore services as quickly as possible and in compliance with service levels agreed with the business. In addition to technical considerations, the human factor is often the weakest link when it comes to cyber security. Irrespective of the technologies and controls in place, if an employee is not willing to take responsibility for cyber-secure practices, then this exposes the organization to even greater cyber security risk.

Expo 2020 selected the Cyber Smart programme from Digital14 with the aim of incorporating a thorough cyber security awareness program that will establish an intelligent, cyber-smart team capable of ensuring the data of all visitors and international participants is safe and secure. All employees and partners will undergo relevant training, which will in turn be invaluable with regard to maintaining safety and cyber security.

Expo 2020’s cyber security team is organized to provide a comprehensive cyber security service covering infrastructure networks and application security, monitoring and operations, and compliance and governance. Alongside a specialized team of cyber security experts, all Expo employees will ensure operations related to the event are aligned with the highest standards of cyber security. To encourage this, Digital14 and Expo 2020 initiated an information security cyber awareness campaign ‘Cy Safe’. The campaign targets different segments of Expo through a novel, interactive set of learning modules that can be easily shared with partners and staff.

Expected Outcomes
World Expos are widely regarded as catalysts of social and economic transformation that generate enduring impacts for host cities and nations. Promising to deliver a safe and secure digital experience like no other, Expo 2020 Dubai is set to create a lasting legacy for visitors, participants, and the UAE – underpinned by world-class cyber security innovations.

With the ever-growing adoption of connected devices globally, digital platforms will help shape each visitor’s experience of Expo 2020 – making cyber security crucial to the success of the six-month event. Working hand-in-hand with Digital14, Expo 2020 Dubai is on track to deliver one of the most technologically secure World Expos in history.

CASE STUDY: EXPO 2020 DUBAI
In its review of the current and most active threats targeting IoT devices, Digital14 surveyed the attack surface within the UAE through open-source research to ascertain the risks facing organisations in the country. Digital14 specifically reviewed public-facing hosts that can be easily breached by the army of existing botnets and examined current IoT attacks on compromised devices in the region.

As compared to other GCC member states, the UAE is at a particularly high risk of attack, given the large number of publicly-exposed devices commonly targeted by IoT botnets. The adoption of Smart City initiatives will certainly expand this risk.

An examination of public-facing hosts within the GCC revealed that the UAE has by far the highest number of publicly-exposed devices commonly targeted by IoT botnets. The adoption of Smart City initiatives will certainly expand this risk.

As IoT malware typically operates by mapping and cataloguing public-facing networks in search of commonly vulnerable devices such as IP cameras and DVRs, the graphs indicate that the UAE is now a ripe target for existing botnets to expand their infrastructure. As mentioned previously in the report; these devices are frequent targets of IoT attacks.

Digital14’s examination of global IoT attack data reveals that the UAE is hit by an average of 304 attackers per day – the highest of all the GCC countries (see Figure 11). In this case, attackers hone in on a compromised IoT device within the UAE, and then attempt to target further devices.
With the relatively high volume of IP cameras and DVRs in the UAE and the Mirai malware family’s affinity for such devices, Mirai botnets logically comprise the bulk of all IoT attacks in the country. Nearly three-quarters of IoT attacks are reported in connection with devices compromised by Mirai (see Figure 12). Figure 12. Percentage of Mirai malware variants in IoT attacks in the UAE.

Operators of IoT botnets also often conduct attacks intended to simply expand their infrastructure. Once an IoT device is compromized, the malware tries to use it to attack more traditional public-facing devices. These attacks follow the same technique: they identify potential IoT targets and then scan them for available and vulnerable services. Digital14’s survey looked at compromised services such as webservers and remote access protocols. At the time of writing this report, based on open-source research, 18.46% of public-facing hosts in the UAE were potentially exposed to IoT-based attacks.

Digital14’s first Cyber Resilience Report for 2020 reviews Smart City-enabling technologies and their intrinsic threats and risks for the UAE in its transition to a Smart Nation.

Smart technologies will increasingly enable the convergence of the physical and virtual worlds, and as IoT-related devices and their supporting infrastructure proliferate, threat actors will correspondingly target this expanded attack surface. When everything from power grids to medical devices is connected to the Internet, security could become a matter of life and death.

The UAE has already established itself as a global leader in smart initiatives and technologies. Now the time has come to establish its credentials as a global smart security leader.

Digital14’s research and analysis of Smart City initiatives, as well as the adoption of IoT technologies both locally and globally, reveals an increasingly complex canvas, with an increase in potential threats facing every sector of our society.

This complexity requires increasing levels of cooperation between governments, businesses and citizens. Leaders of organisations that adopt IoT technologies need to prioritise, identify and address the threats outlined in this report. Digital14’s Threat Intelligence capability provides unique insights to clients to enable informed decision-making around the implementation of Smart Technologies while addressing management concerns regarding ongoing and evolving threats. When forewarned against these potential threats, clients are able to enact precautionary measures that protect their businesses while unlocking the efficiency gains of tomorrow’s pioneering technologies.

Digital14’s highly specialised expert teams provide clients with rapid, accurate, and trusted insights into the local, regional and global threat landscape confronting organisations of all sizes. This expertise is applied to protecting the unique, hyper-modern infrastructure of organisations such as Expo 2020 Dubai. With market-leading research and security implementions, the Threat Intelligence Center (TIC), Cyber Network Defense (CND), Security Operations Center (SOC) and Test and Validation Labs (xen1thLabs) collaborate to provide clients with world-class auditing, recommendations and active threat monitoring solutions.
In the newly complex landscape of the IoT-enabled Smart Business, businesses must adopt a number of best practices to protect themselves against new and evolving threats. Digital14 recommends the following security actions to maintain stakeholder trust:

**Validate IoT devices before deployment**

Every organisation seeking to onboard new IoT devices across their enterprise should first test and validate such equipment from the vendor by way of an adequate vulnerability assessment.

Some of the most vulnerable IoT devices, such as routers and IP cameras, are among the most widely used in enterprise environments. The vulnerabilities lie largely in simple oversights such as default credentials, outdated and vulnerable software, or unnecessary and undocumented services to enable administrative access. Indeed, currently observed threats targeting the IoT could be characterised as opportunistic and low in complexity. The Mirai malware family, which accounts for more than 70% of IoT attacks in the UAE, relies entirely on two simple ways of propagation: brute-forcing credentials and leveraging publicly available exploits.

Although usually easily mitigated, such vulnerabilities are even easier to detect and prevent during proper security assessments before the devices are deployed on a wide scale across the enterprise.

**Incorporate IoT devices with risk assessment**

Some IoT devices, such as IP cameras, may not necessarily carry a significant impact beyond their function as access points to identify, read and extolate sensitive data. On the other hand, IoT equipment such as biomedical devices or ICS units could be successfully attacked with catastrophic or even life-threatening results. Regardless of the impact, however, IoT devices introduce significant challenges and differing weights within risk-management processes.

In mitigating risks, IoT devices are not always easy to incorporate into the vulnerability management cycle. Many IoT devices are designed to be low-powered and require minimal computing resources, and therefore may not support the third-party applications needed for security tasks such as patch management. Firmware must be upgraded immediately when made available by its vendors.

**Monitor device activity**

IoT devices can be particularly difficult to monitor with traditional log management systems, as hacking capabilities can vary widely. Nevertheless, most of the active threats detailed in this report – from the wide range of malware strains to the threat actors involved – operated over established network infrastructures. In this regard, network traffic should be monitored for any abnormalities.

Placing security controls such as an Intrusion Detection Systems in line with network-segmented IoT devices can assist in the early detection of IoT attacks or suspicious activity originating from an IoT device. Most botnets, which make up a significant threat by volume, will provide signatures that any capable security operation centre should be able to handle. Automated asset discovery and a network topology mapping system should regularly scan and report its findings on your networks for regular auditing, review and compliance with organisational goals.

**Segment IoT networks**

IoT devices should always be isolated from sensitive consumer and enterprise data. Threat actors such as APTs have already successfully used IoT devices to springboard into broader enterprise networks. As IoT devices are often deployed in greater volumes than critical network infrastructure systems, the attack surface of the network segment is broadened considerably. Similarly, as IoT devices can be more difficult to patch because they are often not designed to support third-party solutions, overall risks associated with the networks would be more difficult to mitigate.

For industrial sites, consider completely eliminating any connections between the IT and OT teams that do not pass through an on-site Demilitarized Zone. Ensure that external connections arrive through VPNs with two-factor authentication. A privileged access control solution should manage credentials. Authentication workflows should be routed in such a way that security operations centres are instantly alerted to any unauthorised access. Finally, develop a granular, policy-based segmentation ruleset to actively control which devices communicate with each other. Such controls are especially critical in industrial environments where traditional security practices may not always work.

**Safeguard data**

Smart City-enabled technology inherently requires the production and storage of enormous volumes of data. Determining the infrastructure and security controls needed to safeguard the data before the technologies are deployed will go a long way to reduce risks of database exposure, such as those seen on a seemingly daily basis.

Unfortunately, data owners do not always deploy the necessary security controls. This is evident by some of the database breaches detailed under Section four. Expanding Risks. According to a survey conducted by Gemalto for its 2018 State of IoT Security Report, only 60% of organisations using IoT technologies encrypt their data. Prior to the launch of new IoT technologies, the sensitivity and location of the forthcoming data must be properly incorporated into risk assessments.

**Regular audits from cloud providers**

Smart Cities’ different components will generate high volumes of data that will require vast quantities of storage. Consequently, some organisations will naturally partner with cloud providers to offload storage and compliance responsibilities.

Since IoT devices often store sensitive personal information about their users, security risk and compliance officers should follow an accepted cloud computing audit assurance program to assess and confirm the policies and controls in use at an organisation’s desired cloud data partner. The Information System Audit and Control Association and the Institute of Chartered Accountants in England and Wales have detailed processes to assist officers assessing risks of various cloud computing environments and ensuring compliance with legal frameworks in their relevant jurisdictions.
Delivering trust in a world where cyber risks are a perpetual threat, Digital14 guides clients on their journeys to reach unprecedented heights and navigate what lies ahead in tomorrow’s digital frontier. Digital14, established in 2019, is wholly owned by ADQ, a public joint stock company, holding a diverse portfolio of major enterprises spanning key sectors of Abu Dhabi’s economy. This base provides the ideal platform for Digital14 to accelerate digital advancement and cyber resilience solutions via robust, end-to-end solutions. Whether it is enjoying the freedoms of a protected internet, secure transactions or safe communications – we Protect, Transform and Nurture today so that everyone can flourish with the freedom to achieve their potential, tomorrow.

For more information, visit https://digital14.com