Security by Design

Safe and secure smart cities in a volatile cyber world

EY
Building a better working world

WORLD GOVERNMENT SUMMIT 2021

Table of contents

Topics

01

Foreword

By 2050, 70% of the world's population will live in urban areas. Catering to demands of this ever-increasing population in cities, and impact on business operations will require innovative methods and digital solutions to accomplish this. Furthermore, governments across the world expect cities of tomorrow that are smart, technologically connected and sustainable to assist in delivering an enhanced lifestyle, and create new ecosystems across all sectors including food, water, energy and more.

While smart cities continue to invest in emerging and disruptive technologies to develop sustainably and navigate the new era of resident demands, such rapid digitalization presents an opaque universe of cyber threats that may cause significant harm. Therefore, smart cities and governments across the world need to analyze security requirements, and invest heavily in securing information and communication technologies, including all digital services, while increasing cyber awareness among all stakeholders, including residents and government officials.

This paper explores a gamut of topics which are essential for cybersecurity in a smart city including, but not limited to, cybersecurity governance, critical infrastructure protection, evolving threat landscape with digitalization, resident privacy and innovative approaches to offer adequate protection. The research covers both experiential input, global findings around trends, as well as firsthand input from interviewees to ensure we cover the topics from different perspectives.

In light of the numerous smart city projects and cybersecurity programs being undertaken, various subject matter specialists have shared their views on how smart cities must embed a Security by Design concept early in the conception and design phases. This aids to counter cyber threats that continue to plague governments across the world.

In the future, smart city concepts and technologies will no longer be separable from the built urban structure.[1] In order to develop cyber-secure smart cities, it is important to consider the cyber risk and threat landscape, and explore how intersections between COVID-19 and other primary force waves (such as innovative technology) shape the existing and new megatrends for the city. Integration of cyber monitoring and defence mechanisms within city infrastructure should also be carried out to limit the attack vectors and opportunities that attackers can leverage.

Governments across the world need to undertake a series of activities in order to safeguard the digital and critical infrastructure assets of cities from threats and attacks which seem to be imminent at the moment. To stay ahead of threat actors and cybercrime, governments need to be innovative, prioritize assets, understand the risk landscape and implement enhanced level of security controls.

We look forward to exploring this critical area for smart cities in further detail, and performing a deep-dive review of solutions and best practices for navigating the era of rapid urbanization and digitalization of cities through a Security by Design approach.

Latest research estimates global losses from cybercrime to have exceeded

US$1t[2]

1. EY – What does the future of smart cities look like?
2. McAfee and CSIS Report – Hidden Costs of Cybercrime Beyond Economic Impact

02

Executive summary

EY Global Information Security Survey (GISS)[3] 2020 highlighted that 60% of organizations have faced a material or significant incident in the past 12 months, and about one-fifth of these attacks came from "hacktivists" (i.e., tech-enabled, political and social activists) second only to organized crime groups (23%). This showcases the cyber threat landscape that governments across the world need to be aware of. The advent of new technologies, being leveraged across smart city landscapes, provides further entry points for attackers and a risk landscape that is hard to mitigate. Governments presiding over these cities need to embed a risk mindset from the onset of all technology-based projects.

Additionally, urban expansion is adding pressure on smart cities. According to the United Nations, half of humanity (approximately 3.5 billion people) live in cities today. Additionally, 95% of urban expansion in the next decades will take place in the developing world. Expected to house approximately 70% of the world's population by 2050, cities face steep challenges in terms of meeting the demands of its residents. The rapid urbanization and ageing infrastructures are creating significant environmental, social and economic challenges that need to be addressed as soon as possible.

Therefore, cities must enhance their outdated information technology (IT) and system infrastructure as well as traditional service delivery models and governance frameworks in order to achieve its desired outcome (i.e., deliver state-of-the-art services to its residents) and realize its growth potential.[4] If a city were to significantly enhance their infrastructure and leverage emerging technologies, innovative solutions in a sustainable manner that disrupts traditional service delivery and operating models, the city could drive a transformative mindset, that assists it in becoming the successful megacity story of tomorrow.

Within this context, EY defines a city as "smart" when it meets its specific challenges with digital and cross-sector solutions, leveraging information and communication technologies to improve urban processes and services, in terms of public service and sustainability.[5] To counter challenges faced due to urbanization and to manage critical infrastructures in an efficient manner, smart cities adopt a string of disruptive technologies which are often interlinked across sectors, systems and devices.

To operate a vast number of interconnected devices, smart cities require significant collaboration across the three core components of a digital program, which in umbrella terms refers to people, process and technology.

However, the interconnectivity of people, processes and technology within a smart city environment continues to open new vulnerabilities and access points, which cyber criminals are exploiting on a rampant basis. Therefore, governments need to consider the core components that form the basis of the ecosystem, understand the prevalent threats that may cause financial and reputational damage to the city, as well as identify its role in building a cyber-secure environment for the residents.

60%

of organizations have faced a material or significant incident in the past 12 months.

3.5 billion

people approximately live in cities today.

95%

of urban expansion in the next decades will take place in the developing world.

3. EY – Global Information Security Survey 2020
4. EY – Is your city as smart as its residents?
5. EY – What does the future of smart cities look like?

03

What makes a city “smart”?

The smart city concept has been an international trend for several years due to the rapid urbanization and digitalization being observed. This trend can be attributed to the global development of cities.

Smart cities are leading innovative methods of delivering services across all sectors and adopting emerging and disruptive technology to provide a sustainable and digitally enabled future.

There are contradictory approaches to the implementation of smart city concepts, and they differ across regions and sectors. The differing approaches can be attributed to the different challenges that are being addressed by smart concepts, such as population growth within urban cities, geopolitical conditions and demographic shifts.

For a smart city to succeed in its endeavor of delivering innovative and "smart" services to its residents, while safeguarding the digital assets it utilizes, the following three core components which form a smart city need to be considered throughout the transformation program:[6]

1 People

Embedding a risk aware culture across the people ecosystem of a smart city

Smart cities offer residents a platform to share their ideas, collaborate and contribute to "smart" initiatives and obtain a much improved lifestyle that is enabled by digital technologies.

Extensive human interactions within a smart city, including the decisions and actions that arise from them, produce a cohesive outcome that meets the needs of everyone involved within the city. The high level of collaboration also brings about a host of positive impacts, such as innovation, alongside negative impacts, such as cybercrime.

Cybercriminals specifically target residents or employees working in critical infrastructures due to their lack of knowledge around cybersecurity good practices. For example, cybercriminals might target employees with phishing emails designed to get them to click on a malicious link or vishing calls to divulge credentials (including passwords that provide access to critical systems). In such a scenario, it is important to note that smart cities are, at their simplest, collections of individual agents that separately and collectively influence city and infrastructure dynamics. Therefore, each individual agent (including the residents) needs to be aware of the security risks and threats that may impact smart city operations.

Due to the increased participation of residents and laymen in operations, awareness of cybersecurity and IT infrastructure security is critical for all individuals, and regarded as a key success factor for any smart city. Having a centralized body that further integrates cybersecurity into day-to-day operations through threat intelligence, security monitoring, security strategy and security awareness, ensures that a large portion of cybersecurity is covered from all domains and reduces the risk of a threat vector penetrating the smart city infrastructure. This also ensures a top-down approach to cybersecurity, accompanied by a bottom-up approach, wherein residents contribute significantly to innovative ideas and associated security controls.

Cybercriminals specifically target residents or employees working in critical infrastructures due to their lack of knowledge around cybersecurity good practices. For example, cybercriminals might target employees with phishing emails designed to get them to click on a malicious link or vishing call to divulge credentials (including passwords that provide access to critical systems).

6. EY – How resilience thinking can unlock the complexity of urban cities

Case study: Virtual Singapore

"Virtual Singapore" is an example of a city that needs to respond to its strong growth in the shortest possible time.

The city state has about 5 million inhabitants. Measuring digital data with the help of sensors and cameras, the "Virtual Singapore" project summarizes the movements of city dwellers and evaluates them for further development scenarios.

This project is the world's largest data collection for a city. At present, it is not yet clearly defined which service offerings should be generated from this for city residents. In addition, social aspects in the private sphere, such as care of elderly people living alone, are taken into account with the help of sensor monitoring, as well as a more efficient organization of public administration structure.

5 million
inhabitants

Interviewee's perspective

What are the types of cyber resilience mechanisms and methodologies you foresee for smart cities?

Mesfer Almesfer

Chief Information Security Officer (CISO) for a cognitive smart city being developed in the Middle East region

Create independent hardwired systems, not connected to the internet for the control of vital urban infrastructure

Create independent electrical systems for military bases and other critical facilities

Review and upgrade the critical national infrastructure security

Engage in systematic security training for all residents and key personnel involved in managing systems and confidential information

Improve processes and regulations to detect report and respond to cyber attacks

Implement comprehensive data protection governance structures and policies

2 Process

Minimizing cyber attacks using efficient and effective cybersecurity processes

Although it is practically impossible for a city to be fully cyber-secure, establishing the right set of policies and processes for cybersecurity assists in reducing the risk of a successful cyber-attack.

First and foremost, smart cities need to establish a cybersecurity strategy that considers the needs and requirements of all sectors, and places an increased level of focus on critical infrastructures. The strategy document should further drive the processes to be defined and consistently followed.

From a smart city perspective, the following processes are of essence due to the value they hold in terms of mitigating cyber threats.

Build and rehearse resilience capabilities

For a smart city to respond to a security incident or event, an incident response plan needs to be established to provide repeatable procedures and an operational approach to addressing cybersecurity incidents, and to recover business processes as quickly and efficiently as possible. It goes without saying that the rehearsal of the plan is what will make it work.

Understand the risks and threats

Understanding the risk and threat landscape is another critical element of cybersecurity within smart cities and needs to be considered as a key focus area. Threat intelligence may reveal specific attacks that cyber criminals are carrying out using security gaps or vulnerabilities. Armed with this information, security teams may implement additional security controls and countermeasures (e.g., modifying system configurations) on a proactive basis. Therefore, security teams must document detailed processes for collecting threat vector details from a variety of sources, validating and corroborating the details obtained from multiple sources, and disseminating the information obtained to relevant stakeholders.

High-value asset identification

Protecting every asset is not feasible in today's world due to the nature and complexity of assets being used within a smart city environment, and the sheer volume of digital assets in use. Therefore, smart cities need to consider prioritizing countermeasures based on what matters most to the city — which helps focus investments, while managing the most risk possible. If not performed, a smart city may spend money unnecessarily to protect data, systems, people or processes that are not important to the city. The high-value asset identification requires a thoroughly documented process that guides the sectoral entities within the smart city with regard to the identification exercise.

3 Technology

Adoption of emerging and disruptive technologies to provide state-of-the-art services

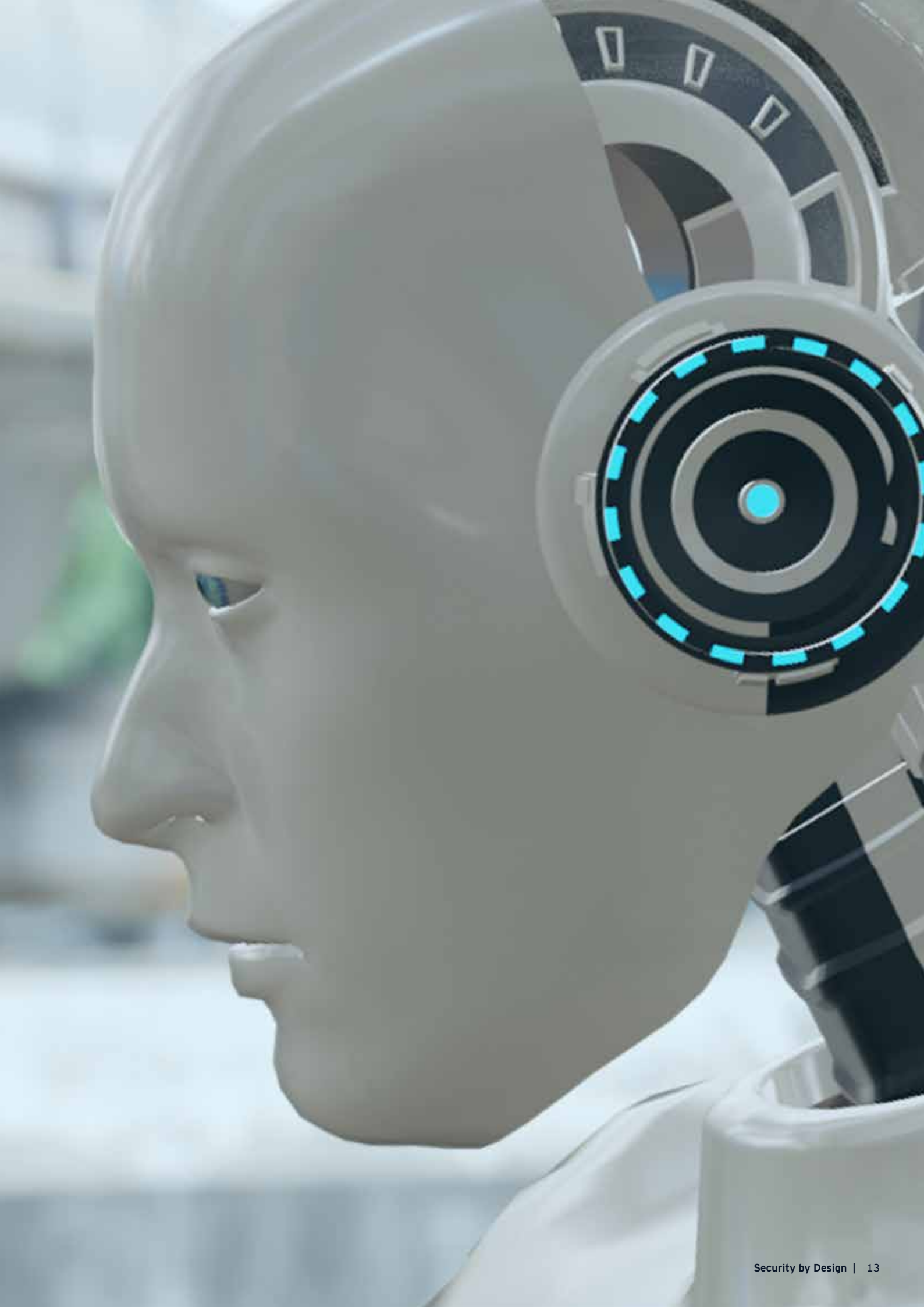
Technology plays a central role in enabling smart cities deliver their intended outcomes. Smart cities quite extensively rely on adoption of emerging and disruptive technologies in order to deliver smart services that shift away from traditional models to new innovative business models.

Taking on many forms, technology can vary from the networks that support the delivery of mobility services, to the IT software and hardware that allow for system integration across the multiple components of a dynamic smart city.

Smart cities utilize data and digital technology to deliver better services, enable ease of operations and processes, and provide opportunities for better decision-making using insights obtained from the data collected from various sensors and devices installed across a smart city ecosystem, among the many benefits it offers. However, the challenge lies in meeting the needs of rapidly increasing number of residents within a smart city due to the large scale urbanization observed across the globe. To meet the needs and demands of a large population, governments adopt highly sophisticated and interconnected systems for offering transportation, power, water and telecommunication services that tend to require a great deal of governance and management, and are generally prime targets for cyber-attackers.[7]

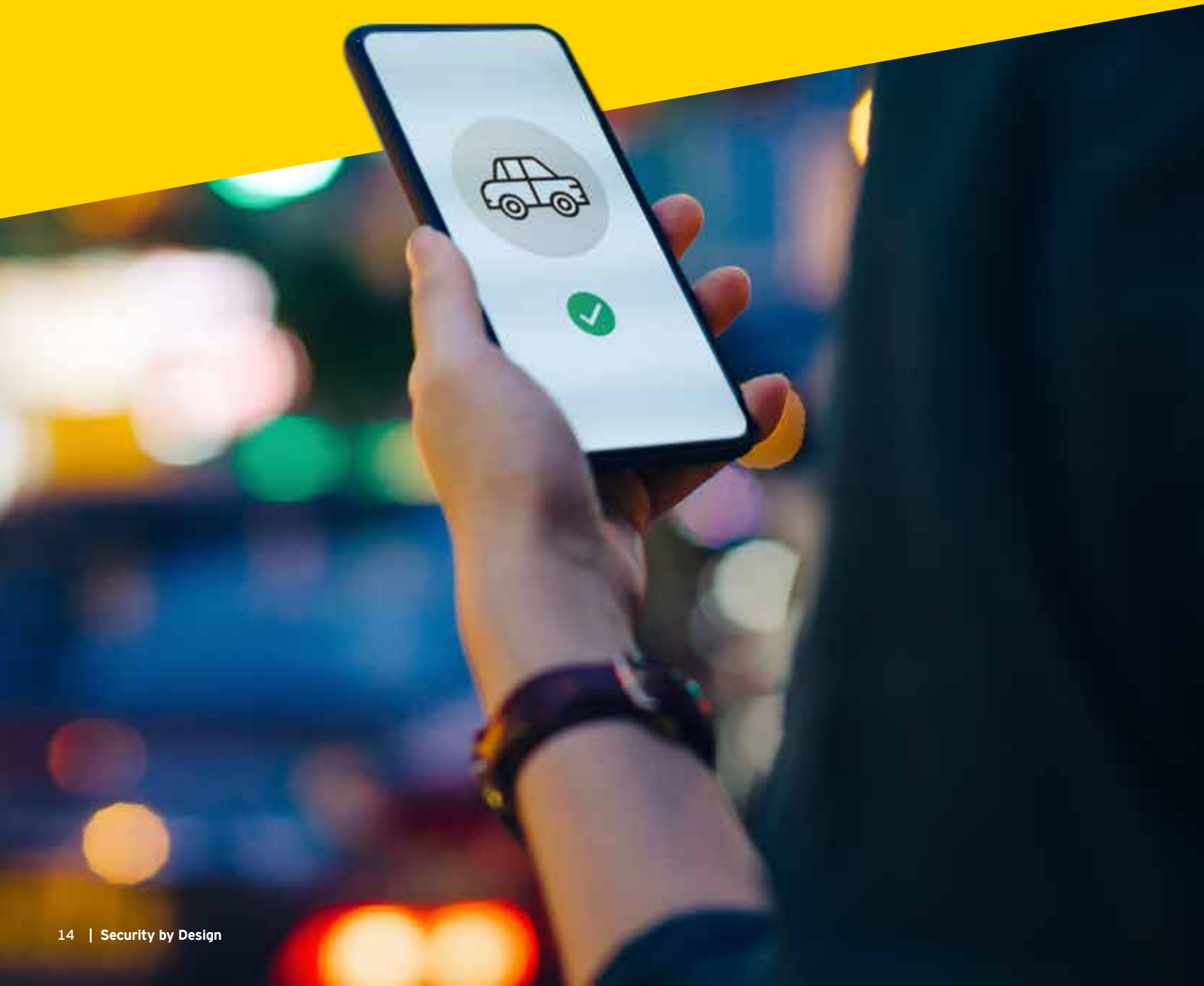
The challenge of embedding security within a smart city ecosystem is magnified due to the extent of damage an attack on a smart city system or network can cause. Imagine a scenario whereby an attacker gains access to traffic control light systems, water supply systems, power and utilities grids – the impact could be far reaching and highly damaging. As a result, governments and smart city authorities need to take a detailed look at the interconnectivity across these three elements (i.e., people, process and technology) in order to build a cyber-secure environment which is capable of mitigating security threats in an efficient manner.

7. EY – How resilience thinking can unlock the complexity of urban cities



04

Disruptive technologies at work



Governments are taking note of the advancements in technology and proliferation of new connected systems and devices. Technologies such as Internet of Things (IoT), and various other forms of disruptors, are offering governments the opportunity to gain more from existing systems using analytics programs and sensors, which have become both cheaper and further advanced.[8]

National-level initiatives

Governments, as part of smart city projects, are harnessing and leveraging cutting-edge technologies to accelerate sustainable development. Examples of such initiatives include use of artificial intelligence (AI) chatbots to improve service delivery, use of big data and analytics to design and implement government policies, and use of IoT and associated sensors to improve decision-making ability by obtaining real-time insights from systems operating critical infrastructures. In short, the use of such technologies has been observed to have improved decision-making ability, and enhance the level of efficiency in city operations while reducing common world problems and challenges.

Benefits

One of the primary benefits of such disruptive technologies seamlessly integrated into an intelligent infrastructure is that it can enable governments to obtain relevant insights, generate intelligence and drive responses to threats or incidents. Advances in intelligent infrastructure offer some of the most exciting prospects. Such infrastructures offer the opportunity to amalgamate modern and disruptive technologies, and form the basis of smart initiatives.

Technology-enabled measures are expected to have equally positive effects in cities around the world, especially in urban areas in Asia, which, along with Africa, is due to see the biggest urbanization growth in the next few decades. A report issued by the GMS Association estimated that Bangkok — infamous for its gridlock and nightmarish traffic jams — could save up to a billion dollars a year by using intelligent transportation systems, which could improve traffic, cut emissions, and boost productivity.[9]

We will be taking a closer look at three disruptive technologies impacting smart cities across the globe, and providing suggestions to embed security during and post implementation of these technologies.

8. EY — Is your city as smart as its residents?

9. EY — Is your city as smart as its residents?

Case study: Barcelona

Barcelona, a city like so many others, was searching for ways to stave off economic and developmental stagnancy following the 2008 recession. To help save money and optimize the urban infrastructure, the local government employed the latest computing technologies and embraced "smart city" initiatives in 12 areas, including water and lighting. This helped reduce congestion and emissions via sensors that led drivers to empty parking spaces; created a sensor network to monitor precipitation and humidity, allowing officials to target irrigation; and installed nearly 20,000 smart meters to measure energy consumption and improve efficiency, among other efforts.

In total, Barcelona calculates that it saved US$37m from smart lighting, US$58m from smart water measures, and increased cash flow from parking by US$50m, thanks to the city's IoT implementation.

Saved

US$37m

from smart lighting

US$58m

from smart water measures

Increased cash flow from parking by

US$50m

1

Internet of things (IoT) and sensors

IoT represents a major transformation in the digital era and has begun to impact every aspect of business and its associated operations. Most IoT devices use sensor-based technologies whereby the sensors identify or measure any change in position, location, etc. The data captured by the sensors are transmitted to a device or server, which in turn is used to analyze the data to generate meaningful information. Smart cities have used several interconnected devices and IoT-based sensors to deliver transformative benefits in a digital era, which include smart life, smart mobility, and smart meters.

Current risks and challenges

However, the vast number of connected devices and cloud computing infrastructures that smart cities are using to be able to deliver results effectively has ultimately resulted in multiplying and ever-evolving cybersecurity challenges. Due to the large number of connected devices, one vulnerable device can lead to other vulnerable devices. This has resulted in attackers having multiple entry points to obtain unauthorized access to city infrastructure and critical systems. Additionally, cloud computing has been a prerequisite for IoT from the very early days of its evolution. However, the lack of security controls implemented within cloud environments that act as a single point of confidential data storage has resulted in various cyber attacks that have compromised security and privacy.

Potential solutions and actions for governments

Governments need to integrate a culture of Security by Design and Privacy by Design in order to consider security challenges and requirements right from the onset. The following elements need to be implemented by smart city authorities prior to wide scale adoption of IoT-based sensors:

- Data protection policies, cloud security standards and guidelines must be established and consistently followed across critical infrastructures utilizing sensors for conducting their operations.
- A multifaceted, defense-in-depth approach is required to ensure the overall security of the smart devices and sensors being utilized.

- The security solutions implemented should be configured to protect the system against evolving threats, by means of a tried and tested near real-time monitoring and response mechanism.

2

Connected cars[10]

The concept of connected cars has moved on from being a mere buzzword to be an area of focus for the automotive industry. Connected cars offer significant benefits such as safety, security and efficiency to various actors involved in the connected car ecosystem. They are also delivering significant customer value through infotainment connectivity, over-the-air (OTA) software updates and autonomous vehicles.

Current risks and challenges

The cybersecurity risks associated with the aforementioned advancements are yet to be fully explored and addressed. Connected cars and mobility platforms that collect a huge amount of data could be subjected to several intrusion and hacking attempts, which could result in compromise of safety features and customer privacy. Additionally, original equipment manufacturers (OEMs) and automotive suppliers are facing challenges with respect to complexity of products, managing integrated systems that consist of cloudified networks and applications, decisions regarding usage of 5G connectivity or V2X communications, and an extremely fragmented supply chain. Furthermore, automotive cloud and connectivity spectrums are being targeted by attackers in the form of near field attacks (i.e., a hacker is in close proximity to the vehicle and uses Bluetooth or Wi-Fi to access confidential data) and remote attacks (i.e., hackers target automotive clouds or associated mobile applications to gain access to data or control the connected cars), which is increasing the challenges for securing a concept that lacks regulation and standardization.

Potential solutions and actions for governments

The solution to the challenges being observed with respect to connected cars lies in the form of an approach which considers that the connected car is just one more link in a much wider and complex network. Therefore, a high degree of emphasis should be placed on protecting the complex network (i.e., the interactions between the users or owners of the vehicles and the numerous other actors in the ecosystem). Undertaking this approach ensures that security is looked at in a more holistic manner whereby the overall ecosystem involving systems, platforms and all relevant actors is considered, and the connected car or the associated IoT sensors or actuators are not looked at in silos.

Smart cities' authorities need to consider the risk that unidentified vulnerabilities and zero-day attacks may result in public distrust; therefore, adopt a Security by Design approach. This would mean that smart city authorities would need to define minimum security requirements and baselines for original equipment manufacturers to adopt and implement. Key issues that need to be discussed at a smart city-level in the context of cybersecurity for connected cars include systems used for vehicular interaction, cloud and data storage requirements, protocols to be used for communication, data encryption, user authentication, security trust zones within city networks (based on assurance levels and access controls), protection mechanisms (i.e., security gateways, firewalls), and security monitoring (e.g., command and control centers allowing for remotely controlling connected car networks).

In this regard, smart city authorities have begun collaborating with OEMs and automotive suppliers in order to embed required level of safety and security features within the connected car ecosystem. Furthermore, regulations stated by the World Forum for Harmonization of Vehicle Regulations under the United Nations Economic Commission for Europe (UNECE) will continue to embed cybersecurity within future connected vehicle sales.

10. EY — Cybersecurity and the Internet of Things

3

Smart meter and smart grid[11]

Smart meters and grid infrastructures generate considerable benefits across the energy lifecycle of cities — from power generation through to distribution and consumption. This includes the ability to meet next generation demand response challenges, optimize local grid efficiency, predict power outages before they occur and rapidly restore service, and better inform consumers through real-time availability of energy consumption data.

The grid and smart meter infrastructure appears as a network of networks comprising four core layers, namely physical layer (including coal and natural gas-fired power plants, grid-based renewables, wind farms, nuclear power plants), communication layer (including home area and office networks), system integration platforms (including computing infrastructure) and software systems that allow for data analysis, remote control for load management, device interface integration, etc. These networks tend to be governed by partnerships and market-driven organizations, with an important input and regulation from the government. In order to provide best-in-class services, and enable the smart grids and smart meters to achieve its desired outcome, these partnerships collect a large amount of data, which includes personally identifiable information (PII), that needs to be protected at all costs using sophisticated security solutions and protection mechanisms.

Current risks and challenges

Although the smart meters and smart grids offer significant benefits, cyber attacks associated with such infrastructures can be catastrophic due to the sheer volume of consumers within a smart city reliant on the smart meter system and services. Therefore, if the transition to smart meter and grid energy management is not undertaken with extensive consideration to cybersecurity risks, smart cities may expose themselves to threat vectors which are capable of causing significant financial, reputational and operational damage.

Potential solutions and actions for governments

In order to maintain security of smart meters and smart grids, a comprehensive and collaborative security approach that embeds concepts of Security by Design and Privacy by Design is required, whereby a set of preventive, detective and corrective controls are implemented to ensure the security of the smart metering system. The smart metering system includes end devices, management and monitoring systems, network infrastructure and payment environments. It is also essential that smart city authorities and utility companies consider the integration of supervisory control and data acquisition (SCADA) systems with the smart grids as this would allow utility companies to remotely monitor and control devices within the grid infrastructures for achieving higher efficiency and managing risks.

Some of the key controls necessary to meet the smart grid and metering security requirements are: network segregation (preferably micro segmentation with adjustable trust levels), data encryption (in transit and rest), near real-time monitoring using integration with SCADA systems within a command and control center, device or user authentication solutions, zero-trust models, and device registration or deregistration.

Furthermore, smart city authorities need to establish a fit-for-purpose governance framework, appropriate policies and procedures, continuous monitoring, and a maturity model that shifts from the traditional structures of identifying potential gaps in power and utility infrastructures.

11. EY — Cybersecurity and the Internet of Things

Summary of cybersecurity considerations with respect to disruptive technologies

The aforementioned examples highlight that the numerous advantages of adopting disruptive technologies are accompanied by an immense number of complexities related to interconnected and integrated systems within smart cities. This then creates vulnerabilities which might potentially be exploited by cyber attackers.

Embedding a culture of Security by Design

Governments across the world have significant work to do to embed a culture of "Security by Design," as additional focus and spending on cybersecurity is currently driven by concerns about risk. The EY GISS survey[12] highlighted that spending of many cybersecurity functions is heavily weighted toward business as usual instead of new initiatives, with some organizations spending 5% or less of their organization's cybersecurity budget on new initiatives. This suggests a lack of awareness and focus on addressing an evolving cyber threat landscape at a time when the priority should be investing in new and emerging cybersecurity technologies that are not only capable of reacting to cyber threats and attacks but are also proactive in identifying vulnerabilities and security gaps for improvement. It was also noted that despite growing concern about the exposures that connected devices could bring, just 2% point to IoT-related initiatives as driving new spending on cybersecurity.

Cybersecurity as a key enabler within smart city strategy

Putting cybersecurity at the heart of a smart city strategy is a significant opportunity for refocusing cybersecurity spending. By addressing security challenges that currently plague smart cities, governments and municipalities can help cities maintain and even enhance the trust of residents, regulators and the media. As a start, governments can no longer assume that cybersecurity is solely the responsibility of the information security (IS) or IT functions. Instead, cities must make cybersecurity a core part of the overall strategy and culture. In doing so, they can enable the whole city and its residents to understand the risks they face, embrace the innovation needed to counter those risks, and have the resilience to regroup and restore operations smoothly and efficiently in the wake of a cyber breach.

5%

or less of some organizations' cybersecurity budget is on new initiatives

2%

point to IoT-related initiatives as driving new spending on cybersecurity

12. EY – Global Information Security Survey 2020

05

Security challenges and solutions

The world is witnessing an unprecedented level of urbanization with an estimated 66 cities to have between 5 and 10 million inhabitants, by 2030.[13] While this trend creates great opportunities for cities, it also places great stress on the outdated infrastructure systems that were designed for the needs of a much smaller and less technologically advanced population. This may result in situations where priority is placed on meeting the needs of a constantly increasing population through innovative solutions rather than mitigation of vulnerabilities and security flaws within the existing IT or OT infrastructure.

The rapid urbanization together with ageing infrastructure is creating huge challenges that may have significant consequences. While the urbanization is compelling cities to rethink their strategies and constantly come up with innovative and "smart" ideas, the infrastructure hosting the associated technologies is not being upgraded to support the wide range of differing and interconnected systems.

To ensure sustainable development, information and communication technologies are being used to improve urban processes and services, especially around public services and applying environmental, social, and governance (ESG) sustainability measures. Based on experiences with smart cities across Africa and the Middle Eastern regions, a list of core security challenges for smart cities has been compiled for consideration during a smart city infrastructure implementation and upgrade:[14]

The world is witnessing an unprecedented level of urbanization with an estimated

66

cities to have between

5–10 million

inhabitants, by 2030

13. United Nations – World Cities in 2018

14. EY/India Security Conference/Assocham India – Cyber Security, a necessary pillar for smart cities

Security challenges

1

Insecure hardware

2

Linking vision with strategy and policy

3

Multiple implementation programs

4

Larger attack surface

5

Inadequate funding and financing

6

Lack of standardized security architecture

7

OT infrastructure security controls

8

Deployment of disruptive technologies

Interviewee's perspective

What are the key cyber risks and threats that smart cities may potentially encounter due to adoption of new technologies (e.g., AI, 5G, IoT)?

Mesfer Almesfer

Chief Information Security Officer (CISO) for a cognitive smart city being developed in the Middle East region

I think we are currently at a tipping point with regard to the use of the new technologies. Humans realize the importance of disruptive technologies, however, are reluctant to give up control to machines regardless of what the statistical data may show. Much of this concern comes from a psychological fear of giving up control to machines but the other dimension of this concern comes from a realistic understanding that machine controls can be hacked by cyber criminals and techno-terrorists that could create widespread mayhem if they were able to reprogram machines that control vital systems. Key threats to smart cities come from the following sources or attackers:

Hackers or hacktivists penetrating systems for the purpose of account manipulation, theft, defacement or data destruction

---

Terrorist groups penetrating systems for the purpose of wreaking havoc

---

Nation states penetrating systems for the purpose of espionage

---

Challenge **#1**

Insecure hardware

Problem case

One of the major concerns around smart cities lies in sensor hardware being utilized insecurely and without thorough testing. Owing to lack of standardization of IoT devices, the sensors are prone to hacking. Notorious individuals can hack the sensors and feed fake data, causing signal failures and system shutdowns.

Potential solution

Smart cities need to adopt an approach of incremental upgrades and deployment of emerging and disruptive technologies. This mitigates any negative impact on the IT infrastructure, and ensures vulnerabilities are being monitored and tracked for remediation. Incremental upgrades will assist smart cities in addressing security challenges within the IT infrastructure and ensure hardware components are tested thoroughly prior to large scale adoption of the technology. Additionally, governments could consider establishing common testing criteria and associated laboratories or test beds that serve as security testing facilities, and are accredited to conduct security evaluations for new technology implementations and monitor conformance to industry-recognized standards.

Challenge **#2**

Linking vision with strategy and policy

Problem case

Cities face the challenge of linking the vision for urban transformation with the security strategy and policy environment. Current strategy, policies, and regulations may not align to the new smart city vision established to deliver future city programs – which includes rapid implementation of emerging and disruptive technologies.

Potential solution

Smart cities could consider establishing a working group or committee that is responsible for aligning the overall vision with the security strategy and coordinating cybersecurity activity. Such committees have been implemented in South Africa in the form of a cybersecurity hub, and in the United Kingdom National Cybersecurity Center through the Office of Cyber Security & Information Assurance (OCSIA). The responsibilities of these committees include, but are not limited to, providing continued support on delivery of smart city objectives, confirming delivery of the planned return on investment (ROI) and approving adjustments to the cybersecurity strategy. This will assist in considering needs of all sectors within the city and establishing a strategy that is linked to the future city programs.

Challenge **#3**

Multiple implementation programs

Problem case

Smart city transformation means several initiatives must run in parallel to achieve the planned outcomes. They can have overlapping challenges such as funding and finance, regulatory approvals, and IT infrastructure needs. Due to several initiatives running in parallel, security is often sidelined and does not gain the appropriate amount of traction with key stakeholders involved in the transformation program. These challenges result in potential vulnerabilities left open within the infrastructure, and are often subject to hacktivist and nation-state sponsored attacks.

Potential solution

Security needs to be embedded within initiatives involving technology implementation through a Security by Design approach. Each technology implementation should be routed through a dedicated security team responsible for identifying and assessing security requirements associated with the implementation. The security team should be skilled at performing cybersecurity assessments, and should have a sufficient number of resources to tackle and manage a huge number of projects to mitigate the challenges related to several initiatives running in parallel.

Challenge **#4**

Larger attack surface

Problem case

Smart city operations utilize complex, networked assembly of IT infrastructure to manage the services provided to its residents. Significant number of devices are connected to the smart city network and are vulnerable to being hacked. Therefore, the number of potential entry points for cyber attackers is multiplied in smart cities. By compromising a single device, it is possible to attack the entire system or network.

Potential solution

Smart city operators need to integrate a multifaceted defense-in-depth approach aligned on a kill chain model which protects connected devices against a variety of threat vectors. Furthermore, it is vital for critical infrastructures to implement deception technology (e.g., honeypots, mimicking) by creating traps or decoys to identify a cyber criminal who has managed to infiltrate the infrastructure and prevent the attacker from causing further damage. Around the clock monitoring of the infrastructure by dedicated teams and automated response mechanisms (e.g., security orchestration and automation (SOAR) playbooks) are another critical element to manage a larger attack surface created by the extensive use of connected devices.

Challenge **#5**

Inadequate funding and financing

Problem case

Cities struggle to find the capital for full-scale transformation efforts. Cities lack funds to transition to smart cities with decreasing budgets, competing priorities, and hesitation to invest in large-scale technology and smart infrastructure. The issues with financing smart city transformation result in governments compensating the costs by reducing the amount of investment in cybersecurity.

Potential solution

Governments must consider security requirements and associated costs right from the onset of a transformation program. Transformation efforts should not begin unless the cybersecurity requirements have been identified, assessed and widely discussed across all sectors and key stakeholders. Rather than avoiding risk altogether, smart cities must enable trust in systems, designs and data so that they can take on more risk, lead transformational change and innovate with confidence. This approach requires risk assessments to be conducted prior to deploying a new technology and the influx of disruptive technologies to be appropriately managed by evaluating the impact of deployment on the overall infrastructure. Additionally, cybersecurity should be provided a dedicated budget, rather than having to rely on financing provided to other departments or sectors such as information and communication technologies.

Challenge **#6**

Lack of standardized security architecture

Problem case

Cities lack a comprehensive strategy, security architecture and tools for managing the transformation programs. City systems don't "talk" to one another. There are problems with data sharing, system interoperability and competing priorities. Lack of interconnectivity between city systems and implementation of inconsistent security controls across systems used to manage critical infrastructure has seen several attacks being successfully undertaken by hacktivists.

Potential solution

Governmental entities heading cybersecurity should define the security architecture, and mandate security principles and standards to be embedded into technology implementations. The security architecture should consist of design artifacts, policies, procedures and standards that will assist critical infrastructure operators to understand cybersecurity requirements, and design the technology and IT models in the required manner. Minimum security control requirements should be defined by a central governmental entity to ensure that commonly known vulnerabilities are not present within the infrastructure.

Challenge **#7**

OT infrastructure security controls

Problem case

Operational technology (OT) infrastructure is quite often administered from a generic IT infrastructure which means that the integrity of the OT systems is only as good as that of the IT infrastructure. It has been observed on several occasions that access to OT systems is controlled by a user directory service within the corporate IT infrastructure; therefore, a compromise of the IT infrastructure would result in a compromise of the OT infrastructure used to manage critical infrastructure.

Potential solution

In line with recommendations provided by the National Computer Security Center (NCSC), smart cities should ensure that OT is not administered from a corporate IT infrastructure. This is to ensure that OT systems do not rely solely on systems in a lower trust domain for authentication and authorization. Additionally, smart cities must establish a standardized architecture to help cybersecurity personnel adhere to strict security, compliance, and risk management controls that are consistent across all sectors and allows deviation tracking.

Challenge **#8**

Deployment of disruptive technologies

Problem case

Disruptive technologies such as drones, IoT, blockchain, machine and cognitive learning are adopted pervasively within smart cities. However, the adoption is often driven by enthusiasm, without a pragmatic approach which includes a cost-benefit analysis. While some governments have placed importance on conducting a cost-benefit analysis prior to wide-scale adoption of disruptive technologies, the analysis lacks consideration to expenditure associated with security controls to be implemented, in order to protect the technology implementation.

Potential solution

Governments should mandate the deployment of a well-defined cost-benefit analysis, which includes considerations to security requirements for disruptive and emerging technologies. The cost-benefit analysis should be supplemented by extensive research and development activities, with respect to security controls associated with pioneering technologies that may not have previously defined security standards (e.g., green hydrogen, flying cars, contactless delivery through drones).

Smart city transformation programs are typically undertaken with limited resources, minimum financing and a lack of common purpose. These disjointed smart city transformation programs are usually associated with limited involvement and participation of cybersecurity functions in the implementation of technologies. The lack of a Security by Design approach may have substantial negative consequences that can have a long-lasting impact on the smart city IT infrastructure. Therefore, governments should take an active role in smart city transformation and technology implementation programs, and embed security into the processes, through well-defined guidelines and security architecture standards that are consistently communicated and monitored across all sectors.

A sustainable and cyber resilient smart city in the digital era

In order to develop smart cities sustainably, it is important that governments take note of the challenges, and deduce customized and contextual security solutions to address the challenges. Failure to adopt security solutions, that are fit-for-purpose from a smart city perspective, may result in limited defence mechanisms which may be exploited by well-trained cyber attackers backed by nation states and terrorist groups.

Interviewee's perspective

What are the risks smart cities expose themselves to by adopting disruptive and emerging technologies?

Dr. Taha Khedro

EY Consulting LLC, Dubai
Leading smart destinations and cities for Ernst & Young in the MENA region and working with EY global future cities

The Internet of Things (IoT) has been observed to have created more vulnerabilities and challenges for smart cities as IoT devices and associated systems require a high-level of protection. The compromise of one device can result in catastrophic damages to vital systems that span a number of critical operations within a smart city. Additionally, the lack of proper planning and consideration to protection of smart city infrastructure has resulted in successful cyber attacks being undertaken on vital smart city systems. Therefore, in this day and age where attackers have become highly sophisticated, utilizing a general security operations center (SOC) will not suffice, and smart cities need to consider implementing a holistic command and control center that acts as the backbone of the smart city operations.

06

Cybersecurity trends

Based on EY teams research, experience and involvement in various smart city projects, we have observed various trends impacting smart cities, which have direct implications in the operations of smart cities and may potentially challenge the infrastructure of a smart city.

Cybersecurity trends	Description
1. IT infrastructure improvement	IT infrastructure improvement is being given utmost importance due to the rapid adoption of digital technologies, innovative solutions for better management of critical infrastructures, and the need to provide smart services to demanding residents, which have a significant impact on a city's IT infrastructure.
2. Rise of megacities	An anticipated surge in number of megacities (i.e., cities with more than 10 million inhabitants), from 33 in 2018 to 43 in 2030.[15] This is increasing the pressure on governments to deliver intended outcomes by leveraging digital and innovative solutions that are pioneering, and do not have a standardized methodology for implementation and management.
3. Demographic shift	Expected dramatic demographic shift with a rise to 2.1 billion residents over the age of 60[16] by 2050, will have a significant impact on health care systems and associated IT infrastructure. As a result, governments will be required to invest heavily in innovative methods for delivering a healthy, vibrant and liveable environment for all residents, including the elderly.
4. Technology implementations	Employing technology to reduce the long-term cost of infrastructure is likely to become only a larger phenomenon in the coming years. By embracing strategies to connect existing infrastructure to digital networks that can make the most efficient use of them, metropolises can save in the present and invest in the future.
5. IoT	Extensive integration of IoTs across the digital landscape is transforming lives for the better and fast becoming the must-have element of business technology. The potential benefits of implementing IoT sensors and systems are far-reaching and governments across the world are implementing IoTs, along with intelligent infrastructure and interconnected networks, and are starting to provide solutions with concepts, such as smart grid, smart waste management, smart traffic control, smart utilities, etc.

15. United Nations – World cities in 2018

16. World Bank Blogs – Are cities ready for their increasingly aging populations?

	Cybersecurity trends	Description
6	Carbon removal solutions	We observe that new carbon removal solutions are emerging for decarbonizing business models, driving long-term value and demonstrating climate leadership.[17] The carbon removal solutions have a significant impact on business models and brings about a host of technological challenges due to the electrification of operations, including transportation, heating and industrial operations, that are generally asset-intensive.
7	Cybersecurity expertise	Governments are investing significantly into building local cybersecurity professionals to mitigate an evolving threat landscape. Recent reports suggest a huge shortage of cybersecurity skills in the market and the only way to address this challenge is through cybersecurity training programs, which begins at the grassroots level. Cybersecurity authorities are also contributing to academia curricula and this potentially signifies that the importance of cybersecurity is well-understood within the industry.
8	Harmonization	A harmonized approach toward managing cyber risks and critical issues is being undertaken through coordination and information sharing between stakeholders of critical infrastructure, governmental institutions, and private sector.
9	Crown jewel identification	Smart cities and nation states have undertaken several projects and initiatives to identify the crown jewels or high-value assets used within the smart city, and enable sufficient level of security controls to protect them from exploitation, breach and unauthorized access.
10	Cybersecurity program refresh	A progression of smart cities is refreshing their cybersecurity program, supplemented by a transition strategy and roadmap, to counter existing stagnant programs which have left them open for exploitation by highly mature attackers.
11	Computer emergency response teams	Computer emergency response teams (computer security incident response units) are mushrooming into action as an increasing number of cities experience a cybersecurity incident.
12	Laws and regulations	Several laws have been enacted by governments to enforce cybersecurity regulations and protect its residents from cybercrime. The laws cover a wide range of electronic activities, and dedicated cybercrime units are used to report and respond to criminal activity over the internet.
13	Agile operating model	A shift toward an agile operating model as disruptive changes in the digital era continue to expand. Cybersecurity authorities operating at a smart city level, are required to constantly evolve their mandate, resource pool, capabilities and partnerships. It is mandatory that the authority is flexible and agile in nature in order to meet the needs and trends of the future as well as provide stable foundations by renovating the core structure.

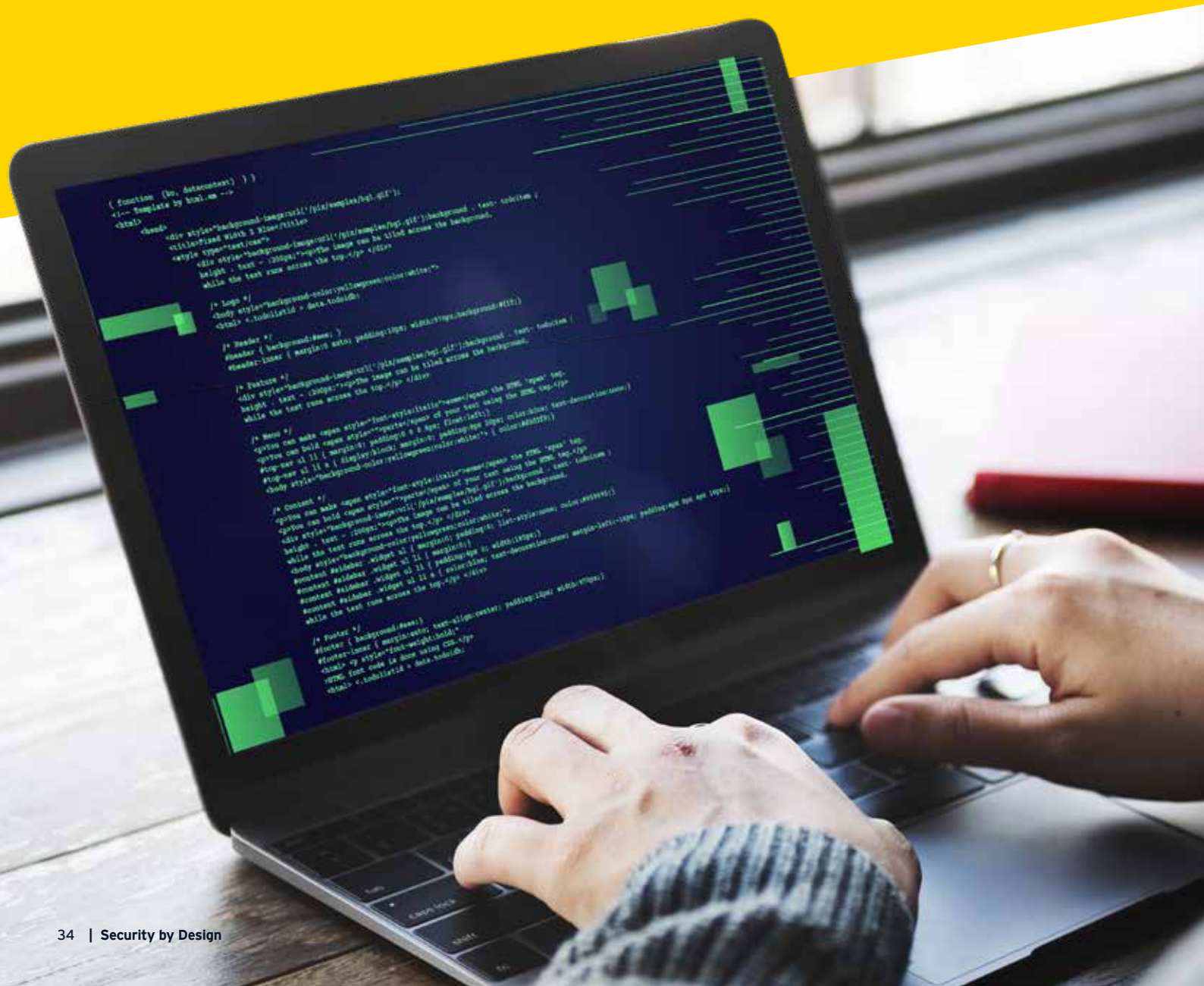
17. EY – megatrends report 2020

Alarming trend observed

The most alarming trend is that the rate at which governments and smart cities across the world adopt digitalization is not equivalent to the speed at which cybersecurity is considered and implemented. A comparison of the Global Cybersecurity Index (GCI) report of 2018 and the United Nations E-Government Development Index suggests that countries that score high in terms of e-government do not necessarily invest in cybersecurity with the same level of commitment and vice versa. Furthermore, a detailed study of the IMD Smart City Index Report 2020, indicates that security is not considered to be the most urgent or priority area for a significant majority of the top-ranking smart cities. This is a significant cause of concern as it signifies that smart cities and associated governments are yet to prioritize cybersecurity efforts that should go hand-in-hand with the overall digitalization and transformation journey.

07

Cyber threat landscape



As the threat landscape continues to evolve and grow, organizations, private institutions and governments across the world are battling cybersecurity challenges. Cyber attacks such as denial of service attacks, man-in-the-middle attacks, and phishing and malware have become common parlance in a world that is adopting digital solutions at an unprecedented rate. The figures speak for themselves. The latest EY Global Information Security Survey revealed that almost half (48%) of all corporate boards believe a cyberattack or data breach will harm their businesses to some extent over the next 12 months. They also think that 40% of those attacks will come from organized criminal groups or social "hacktivists."[18]

This environment makes it challenging for smart cities and governments across the world to pursue digital opportunities, and evolve their business models to increase operational efficiency. In such scenarios, smart cities seeking to enhance their cybersecurity ability need to develop a better understanding of the nature of threats and risks which might ultimately affect them. Smart cities can only enable a secure and resilient environment by identifying the nature of threats and risks which affect them, and by considering how these threats might manifest themselves. Governing bodies of a smart city need to ask pertinent questions to key stakeholders and build discussion forums involving stakeholders, and representatives across all sectors to enhance situational awareness of cyber threats.

Prior to opting for and implementing sophisticated defence mechanisms that safeguard digital assets, smart city authorities need to discuss and consider the types of threats, and the potential impact they may have. Smart cities tend to feel confident about mitigating the various types of attack that have become familiar in recent years (e.g., ransomware, man-in-the-middle attacks), however, the challenge is to counter an ever-evolving threat landscape.

Attackers are getting smarter and using new, evolved and advanced techniques to compromise smart city systems, and gain unauthorized access to confidential information. Unfortunately, smart cities continue to lack capabilities to counter advanced, targeted assaults, especially the ones affecting and impacting the emerging technologies used within critical infrastructures. This is mainly due to the lack of sufficient research and development activities that proactively considers cyber threats during the design phase of a technology implementation plan.

To be cyber resilient, smart cities must constantly quiz relevant stakeholders with regard to the cyber attacks which might affect the various sectors, and consider security risks and threats throughout the lifecycle of a technology implementation. The following table[19] provides three core categories of cyber attacks that plague organizations and governments, and produce a security challenge that seems to keep growing in size and volume on a day-to-day basis.

48%

of all corporate boards believe a cyberattack or data breach will harm their businesses to some extent over the next 12 months.

40%

of those attacks will come from organized criminal groups or social "hacktivists."

18. EY – Global Information Security Survey 2020

19. EY – Cybersecurity regained: preparing to face cyber attacks [Global Information Security Survey 2017-18]

Types of cyber attacks

	Common attacks	Advanced attacks	Emerging attacks
What is it?	Attacks that exploit known vulnerabilities using freely available hacking tools, with little expertise required to be successful	Attacks that exploit complex and sometimes unknown (zero-day) vulnerabilities using sophisticated tools and methodologies	Attacks that focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities
Typical threat actors	Unsophisticated attackers such as disgruntled insiders, business competitors, hacktivists and some organized crime groups	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation states	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation states
Examples	▸ Unpatched vulnerability on a website, exploited using a freely available exploit kit ▸ Generic malware delivered through a phishing campaign, enabling remote access to an endpoint ▸ Distributed denial-of-service (DDoS) attack for hire with a basic random demand	▸ Spear phishing attacks using custom malware ▸ "Zero-day" vulnerabilities exploited using custom-built exploit code ▸ Rogue employees "planted" to undertake deep reconnaissance or espionage ▸ Vendors or suppliers exploited as a way to gain access to ultimately target the smart city	▸ Exploiting vulnerabilities on "smart" devices to gain access to data and/or control systems ▸ Leveraging security gaps created with the convergence of personal and corporate devices into one network ▸ Using advanced techniques to avoid detection and/or bypass defense

It is important for smart cities to note that contrary to popular belief, many cyber attacks do not occur for monetary gain. According to the United Nations, online human trafficking, digital espionage, and cyber attacks on critical infrastructure are potent digital age challenges perpetrated by individuals and groups operating in a borderless virtual realm.

Cyber attacks on critical infrastructure have been observed in the past, whereby attackers have managed to bring supply chain and manufacturing operations of a city to a complete standstill. The NotPetya ransomware incident in Ukraine is one such incident where a nuclear power plant was subjected to a cyberattack, whereby the radiation monitoring system at Chernobyl was infected with malware, forcing manual control.

Among the critical infrastructures including electricity, gas and water supply systems, cyber attacks on electric power systems have recently been reported at an increasing rate. The primary cause of these attacks seems to rest in the industrial control systems (ICS) and SCADA systems that are extensively used in order to improve system maintenance efficiency, and reduce the costs of critical infrastructures. Unfortunately, the complex OT brings about a heightened level of risk alongside the benefits. These OT platforms act as a gateway for attacks that permit intrusion of the control systems using malware infections. As a countermeasure to such risks, critical infrastructures have been operated without connecting their control systems to external networks, including the internet.

Such cyber attacks underline the need for smart cities to relook at their strategies and defence mechanisms to better counter cyber threats impacting control systems. It is important to bear in mind that an attack on a critical infrastructure may result in a significant financial, operational and social impact as well. Therefore, in order to better counter cyber threats and attacks, smart cities need to undertake a series of steps that evaluate the cyber threats and build a threat profile of an attacker, prior to implementing countermeasures.

Actions to be undertaken to counter an evolving threat landscape

Perform proactive and periodic cyber risk assessments

Perform proactive, structured and "context-aware" cyber risk assessment with knowledge of:

- Operational and technical processes, including those conducted within critical infrastructures such as food, water or energy
- Systems and applications utilized for service delivery
- Underlying IT infrastructure, networked components and interconnected devices
- Traffic patterns across the network that provide visibility into anomalous activities conducted by a threat actor
- User activity (traceability tests, system logins)

Undertake 24x7 security monitoring of the IT and OT infrastructure

Conduct security monitoring at all levels:

- Authorities and all governmental entities must understand current security posture of the cyber security environment
- Establish granular controls for hosts, network and end-point parts of the cyber security infrastructure
- Establish capabilities for near real-time security monitoring of the cyber security environment by utilizing a holistic command and control center (i.e., assisting in managing cyber-physical systems, and undertaking efficient and timely response to threats or attacks)

Establish and implement incident response plans and capabilities

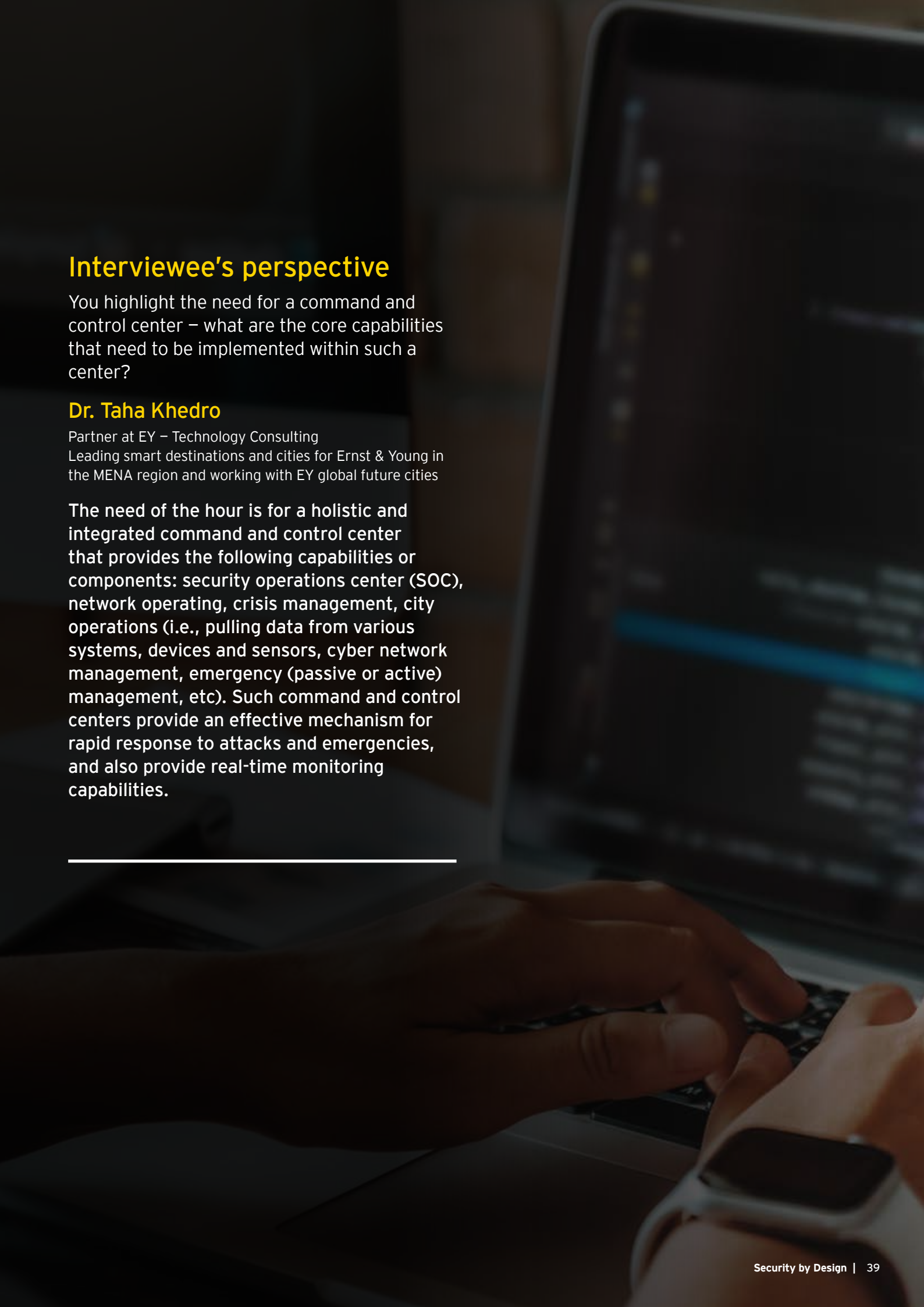
Create or improve a cybersecurity incident response plan:

- Document updated escalation points and incident response contacts
- Establish post-breach detection activities (triage)
- Establish detailed incident response plans that include roles and responsibilities for relevant stakeholders and a cross-functional team
- Conduct simulated exercises and test-drills across the critical infrastructure
- Establish a data privacy office (DPO) that performs data collection, data consent management and handles personal data disputes

Conduct independent reviews of the cybersecurity program

Adopt more stringent control processes:

- Conduct cybersecurity audits to cover all components of the cybersecurity environment – beyond application and general controls
- Perform independent technical security reviews and penetration testing or attack-simulation exercises on a periodic basis by involving all relevant stakeholders operating the critical infrastructures
- Enhance security log data collection and storage process (e.g., commit all cybersecurity logs to another server)



Interviewee's perspective

You highlight the need for a command and control center – what are the core capabilities that need to be implemented within such a center?

Dr. Taha Khedro

Partner at EY – Technology Consulting
Leading smart destinations and cities for Ernst & Young in the MENA region and working with EY global future cities

The need of the hour is for a holistic and integrated command and control center that provides the following capabilities or components: security operations center (SOC), network operating, crisis management, city operations (i.e., pulling data from various systems, devices and sensors, cyber network management, emergency (passive or active) management, etc). Such command and control centers provide an effective mechanism for rapid response to attacks and emergencies, and also provide real-time monitoring capabilities.

08

Security by Design: Key considerations for governments

New technologies such as AI, biotechnology, machine learning, big data, quantum computing and 5G are being extensively utilized to offer smart services to residents of smart cities. Advancements in technology have resulted in smart cities transforming previously analogue processes into digitally enabled processes and have substantially improved the lifestyle and well-being of residents and the workforce used to manage smart cities.

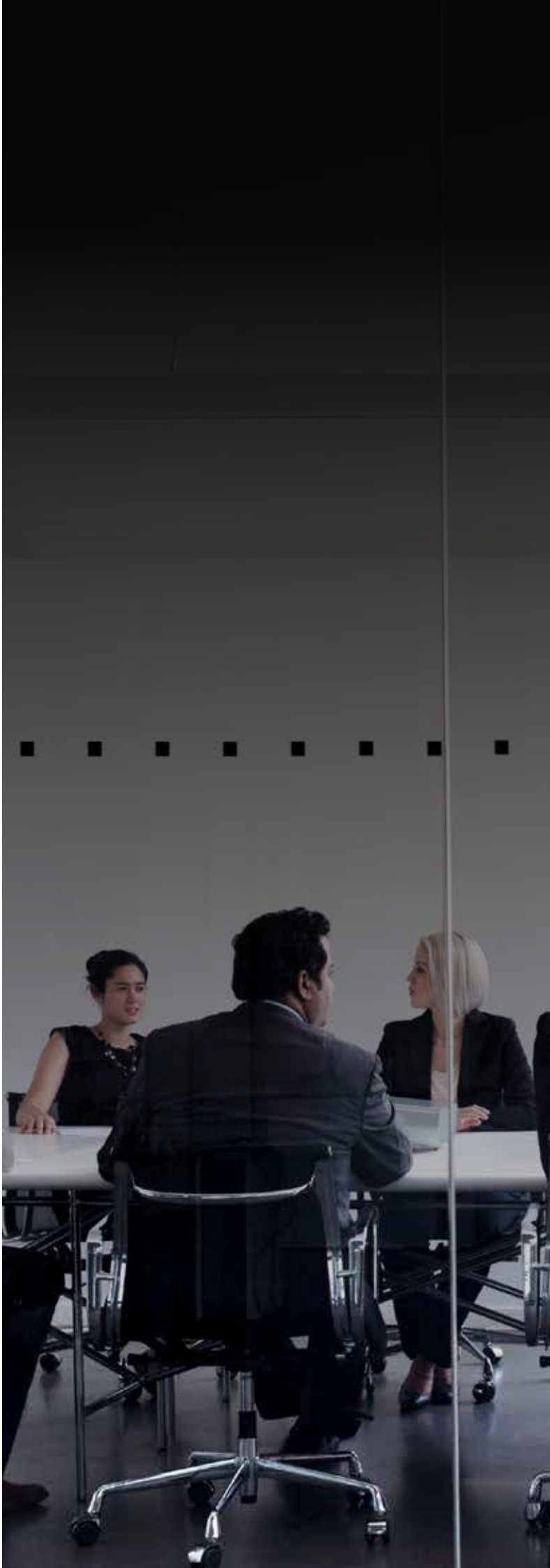
Smart cities have also begun extensively utilizing quantum computing to assist with the validation process of smart city devices and increase the speed of verifying these devices. This is enabled by the fact that quantum computing allows for storage of large volumes of data and allows easy transportation across various interconnected networks within a smart city infrastructure. Quantum computing has found multiple use cases within a smart city which include, but are not limited to, optimizing city-wide traffic flows and electrical grids. This will force governments to rethink their security approaches if used or targeted by the attackers.

Some of the advanced smart cities are also using interconnected systems which offer a single source of data consolidated from multiple systems to enable data-driven decision-making and obtain relevant insights to manage critical infrastructures. For example, smart cities in the Middle East region have begun implementing advanced Internet of Water (IoW) to completely connect the water distribution network using an advanced and integrated infrastructure in order to ensure minimal water loss.

However, this integration and interconnection of multiple systems require cooperation on an organizational, procedural, commercial, legal and technical level. It is imperative for smart cities to ensure that appropriate integration of technologies into the city design and structure is considered throughout a transformation program, or during the establishment of a new infrastructure.

Furthermore, smart cities need to understand that integration of new technologies and multiple interconnected systems are seen as an excellent opportunity for damage by hacktivists and other types of cyber attackers. The rationale for this lies in the fact that attackers have access to multiple entry points, which ultimately leads them to a single source of data. Therefore, compromising one system will lead to unauthorized access to millions of records, including personal information such as names, addresses and social security numbers.

The key to an efficient and effective smart city rests in the ability to provide cross-sector solutions and IoT platforms that are user oriented, and provide enhanced administrative process for smart city operations.



Interviewee's perspective

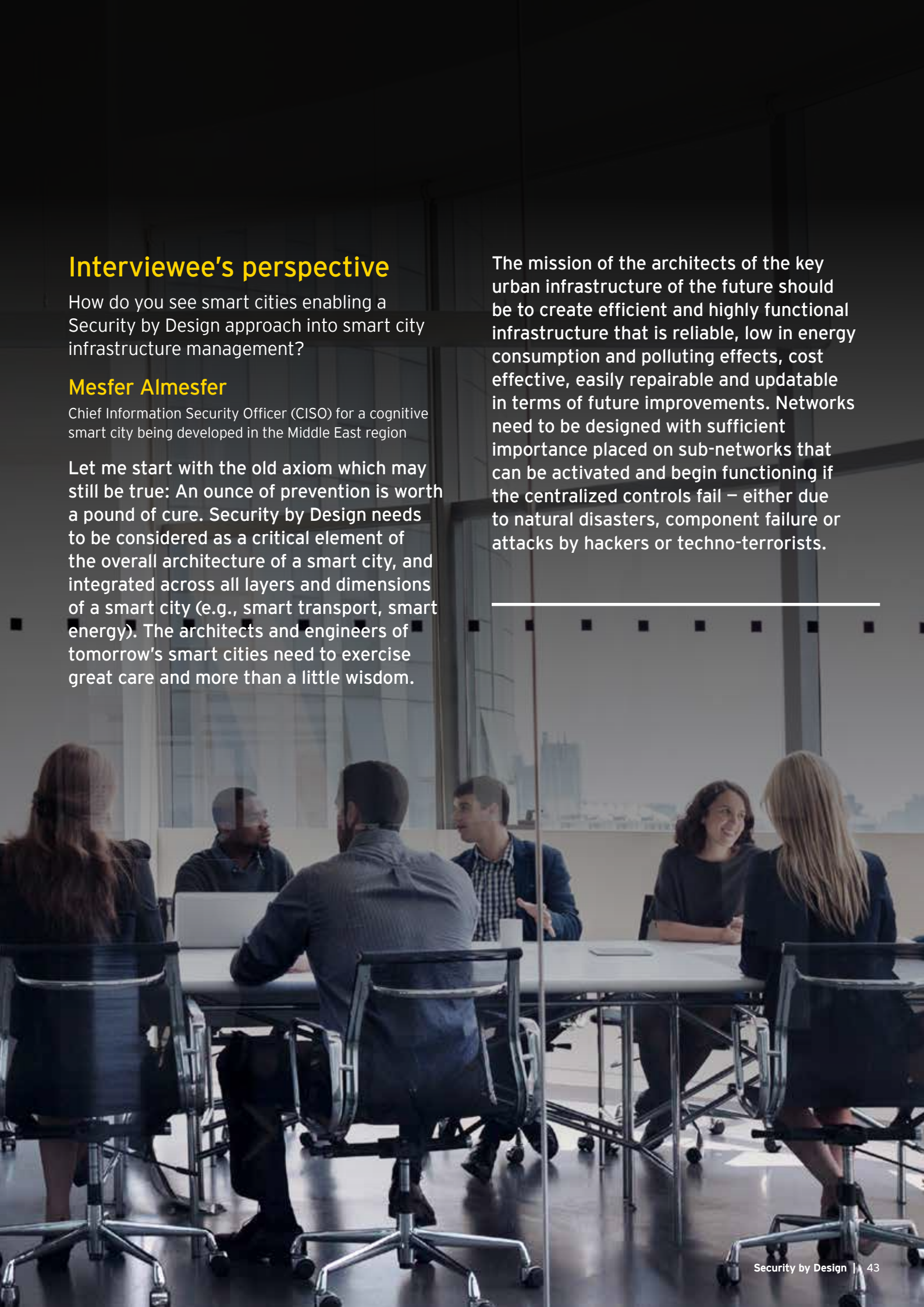
How do you see smart cities enabling a Security by Design approach into smart city infrastructure management?

Mesfer Almesfer

Chief Information Security Officer (CISO) for a cognitive smart city being developed in the Middle East region

Let me start with the old axiom which may still be true: An ounce of prevention is worth a pound of cure. Security by Design needs to be considered as a critical element of the overall architecture of a smart city, and integrated across all layers and dimensions of a smart city (e.g., smart transport, smart energy). The architects and engineers of tomorrow's smart cities need to exercise great care and more than a little wisdom.

The mission of the architects of the key urban infrastructure of the future should be to create efficient and highly functional infrastructure that is reliable, low in energy consumption and polluting effects, cost effective, easily repairable and updatable in terms of future improvements. Networks need to be designed with sufficient importance placed on sub-networks that can be activated and begin functioning if the centralized controls fail — either due to natural disasters, component failure or attacks by hackers or techno-terrorists.



In the following section, we take a look at key considerations for smart city authorities and governments. These considerations provide a detailed view of critical elements that have been impacting smart cities and the areas that need to be addressed. In order to maintain an efficient and resilient smart city, appropriate management of the below-mentioned considerations is paramount and governments need to embed these within the various strategies it establishes.

The considerations covered in this paper, include the following:

1 Interaction and collaboration

2 Big data and predictive analytics

3 Testing environment

4 Security architecture

5 Zero trust and micro segmentation

6 Physical security

7 Public-private partnership

Consideration #1

Interaction and collaboration

Our experience across the regions of Africa and the Middle East suggests that smart cities feel that their cybersecurity functions are stuck in defensive mode – not yet ready to play a central role in enabling the business to transform.

The EY GISS survey[20] provides a grim picture of the existing reality and underlines the current issues organizations are presently facing with respect to building meaningful relationships with the various sectors and departments to tackle security challenges.

The GISS survey reveals that

72%

of organizations say the relationship between cybersecurity and marketing is at best neutral, to mistrustful or non-existent;

54%

say the same of the research and development team;

51%

for the lines of business. Cybersecurity teams even score poorly on their relationship with finance, with whom they are dependent on for budget authorization;

56%

of companies say they fall short. In such a scenario, cybersecurity is perceived to be a roadblock to transformation projects, rather than a key enabler, helping smart cities to innovate with confidence. Therefore, while designing smart cities, it is imperative for governments to reach out to the various sectors and functions, and mandate regular interactions for working closely than before.

20. EY – Global Information Security Survey 2020

Consideration #2

Big data and predictive analytics

It is equally important for governments to look at their data collection and gathering practices due to the significantly huge potential for gaining insights from data collected from various sensors and devices operating within a smart city. Big data management is a critical component of smart city infrastructure management. It provides a systematic way to analyze and deal with data sets that are often large and complex in nature. Appropriate data management practices, accompanied by predictive analytics, have been used extensively by smart cities. They proactively identify customer requirements, enable future-designed decision-making and extract valuable information for improving resident well-being. Essentially, what we are referring to indicates data-driven smart cities that utilize the data collected for efficient handling of smart city infrastructure, such as smart meters, smart lighting and waste management.

With the advancement of emerging technologies such as Internet of Water for ensuring minimal water loss, data is being used to its fullest potential in order to automate the water management processes. Municipal transportation systems are leveraging big data to optimize routes and schedules, decrease traffic congestion, and increase environmental friendliness. Big data analytics and historical data is helping in reducing accidents. By analyzing the history of mishaps, traffic authorities get the cause of the accidents to prevent them in practice. Additionally, asset-intensive sectors such as power and utilities have seen the rise of smart infrastructure such as smart grids, smart water and smart energy. The rapid distribution of smart grids has enabled analysis of real-time power generation and consumption data. The analytics of power usage habits of citizens and industrial objects can help predict the need for power supply in the future.

As observed, big data is collected and gathered from several OT systems, and is used to manage critical infrastructures. This further highlights the need for governments to ensure that sufficient level of security controls is applied to repositories where such information and data get stored, as the compromise of these repositories or databases might result in catastrophic damage. Hackers in the past have been able to compromise smart city systems and databases, bringing critical infrastructure operations to a standstill.

The challenges with gaining relevant insights from the data collected from sensors and connected devices often rest with the raw data being collected, rather than the analytics platforms associated with it. The data is stored in disparate systems and in formats that differ from each other. Analytics platforms are not able to function at their highest capabilities due to the lack of consistent data, resulting in inaccurate or false information being generated — impacting decision-making. Therefore, smart city design needs to consider big data management right from the onset and create the data flow architecture for the data sets to be fed into the analytics platforms.

Additionally, cities increasingly utilizing centralized repositories for interlinking data collected from multiple city systems and maintaining a centralized source of data. However, the interconnectivity across virtual and physical infrastructure that makes a smart city work also has its downside in cybersecurity risks. Smart cities are vulnerable to numerous cyberattack techniques such as remote execution and signal jamming, malware, data manipulation and DDoS attacks.

Connected devices should be protected by comprehensive IoT security solutions. Furthermore, secure boot technology should be utilized to prevent hackers from replacing the firmware with malicious versions, thereby preventing cyber attacks.

Asset-intensive sectors should ensure that a smart device being connected to the network is authenticated before receiving or transmitting data. Unverified devices need to be extensively sandboxed and analyzed prior to being connected to the OT network which generally caters to critical infrastructures. If security violations such as malware or vulnerabilities are observed in the connected devices or associated data, IT functions of smart cities should take proactive action to quarantine the devices based on anomalous behavior.[21]

21. Analytics Insight — Futuristic smart cities: Are they guarded against cybersecurity threats?

Consideration #3

Testing environment

Smart cities adopt digital technologies and IT assets to provide much more efficient and effective services to residents. The solutions are often innovative and "new" as they have not been extensively used in the past. In such a scenario, it is obvious that vulnerabilities associated with the new and disruptive technology will not be known to the authorities implementing them. Therefore, it is vital for smart cities to test and scale any new technology prior to connecting it to the IoT, IT or OT networks. Smart cities and municipalities have begun adopting this approach as observed in Vejle Municipality, Denmark. Vejle Municipality tests and scales new technologies that can create cleaner, smarter and more climate-friendly urban spaces.[22]

Smart cities have been utilizing test beds to perform security and functional testing on connected devices and IoT sensors. For example, Kista Science City, the reality lab of Urban ICT Arena, has real people, with real buildings, real traffic and real conditions, along with a dedicated testbed. All the necessary infrastructure for testing has been established, and the testbed is ready for plug and play, which is ideal for testing smart city devices such as sensors and hardware.[23]

Smart city governments need to mandate the usage of such labs and testbeds across all sectors, especially critical infrastructures, prior to implementing a new technology, system, device or asset within the smart city infrastructure or environment. This will assist IT functions in identifying potential security gaps and vulnerabilities that may need a heightened level of security control to keep attackers at bay.

22. Global Opportunity Explorer – testing and scaling new technology to create a smart city
23. Smart City Sweden – Urban ICT Arena – Testbeds for digitalisation in an urban environment
24. EY – What does the future of smart cities look like?

Consideration #4

Security architecture

Smart cities should publish architecture standards that govern the configuration of all systems, regardless of risk rating and the sector. A dedicated architecture function should evaluate the relevance of developed standards, update and create new standards as threats and risks evolve. It is important that the architecture function performs continuous monitoring of standards compliance. Furthermore, dashboards should be made available to publish reports summarizing noncompliance issues detected with architecture standards. Real-time detection and reporting of noncompliance instances is being performed by cities in order to reduce lag time.

Smart city architecture should be based on five integrated levels:[24]

1. Built city structure (streets and buildings)
2. Infrastructure network with technical facilities and equipment
3. Collection and combining of data
4. IT platforms that process third-party data and prepare it for applications
5. Resulting service offers that are put in place for the users

Integration among these levels and associated security standards should be of primary concern to smart city operators. The value from data and information collected across sectors is dependent on the infrastructure network being linked to the IT platforms, applications in use, and the overall security outlook. This ultimately results in the right kind of services being offered to users and residents, and allows city infrastructure to be managed in an efficient way.

Consideration #5

Zero trust and micro segmentation

Organizations and governments in general are adopting a zero-trust model — a security concept that requires all users (including the ones within the critical infrastructures and government) to be authenticated and authorized, and the security posture to be continuously validated prior to granting access to critical systems and applications. Smart cities will need to be diligent and further strengthen the zero-trust approach by implementing a network defense perimeter. Considering the number of potential connected devices required within a smart city model and the number of potential vulnerabilities, smart cities should add micro segmentation to their security arsenal. Micro segmentation allows cities to separate and create barriers that help contain any potential threat, stopping a bad actor or a single infected device from compromising other services.[25] Additionally, governments should consider establishing separate trust zones within the network design and architecture for systems that are associated with critical infrastructures. The idea behind such a setup is to ensure that OT or IoT technologies and systems that generally cater to critical infrastructures such as energy, water, and power, are linked to a heightened level of security controls than the level provided to generic IT networks.

The architects and engineers of tomorrow's smart cities need to exercise great care and more than a little wisdom. The mission of the architects of the key urban infrastructure of the future should be to create efficient and highly functional infrastructure that is reliable, low in energy consumption and polluting effects, cost effective, easily repairable and updatable in terms of future improvements.

Consideration #6

Physical security

The physical security of a smart city's information processing facilities and data centers is paramount, as they house critical data used to operate smart city infrastructures.

Surveillance cameras are extensively used in smart cities for the purposes of policing and identifying anomalous behavior. It can be challenging for monitoring teams to perform their duties 24x7, and efficiently review, process and analyze countless hours of video footage generated by hundreds — sometimes thousands — of cameras in a smart city. Fortunately, AI-based video content analytics can effectively and accurately deliver both granular information — such as persons and objects of interest — and general trend data for maximizing operational efficiency.

Smart cities need to combine AI with physical security systems, such as badge-reader systems and closed circuit television (CCTV) systems. Any instances of shared tenants must have detailed bifurcations that are protected by cyber-physical systems, and need to be tracked and monitored on a continuous basis.

25. IIoT World — Use a Zero Trust Approach to Protect Your Smart Cities Projects from Hackers

Consideration **#7**

Public-private collaboration

Public-private partnerships (PPPs), as defined by the World Bank, are typically medium to long-term arrangements between the public and private sectors, whereby some of the service obligations of the public sector are provided by the private sector, with a clear agreement on shared objectives for the delivery of public infrastructure and/or public services. Employing PPPs to mitigate funding and skills gaps is a potential solution to infrastructure and environmental challenges, one that has been successfully tested in the UK, Australia and Canada.[26]

The private sector can help governmental institutions and public sector organizations to mitigate the challenges of rapid urbanization. Therefore, while designing a smart city, governments need to consider the collaboration model with private sector enterprises and define the approach for leveraging private sector skill sets. Smart PPP contracts, including the use of smart technologies, may be established in smart city projects such as the installation of a network of sensors or the development of open data policies, data leakage protection, as well as analyzing and mitigating cyber threats.

The documented whitepaper based on the Uraía Workshop[27] suggests that the local government may partner both with big service and technology providers, as well as with small and medium-sized local firms or start-ups. Smart PPPs may involve comprehensive reforms of the legislation and procurement procedures. There is a wide range of legal arrangements available for the different parties to enter into a partnership for better implementation of secure smart cities.

26. EY – Is your city as smart as its residents?

27. Uraía – Public-Private Partnerships for SMART City Management

09

Government's role

Governments have a central role to play in future cities providing smart products and services and developing a digital economy. Governments must engage and incentivize private businesses to help deliver the necessary infrastructure, train a digitally literate workforce, and enable secure access to digital services.[28]

Infrastructure housing the interconnected devices and systems forms the basis of any digital transformation journey. The infrastructure must be continually improved, in line with technologies being adopted and implemented. However, merely updating the infrastructure to accommodate disruptive technologies will only lead to a significant number of security challenges. Therefore, the goal of governments should be to build a reliable and secure infrastructure that has sufficient security controls and processes to safeguard the smart city assets.

Recent times have seen a trend in governments appointing a central authoritative entity, at the smart city or national level, which has the mandate to define, enforce and regulate cybersecurity guidelines. Governments have quite often adopted a centralized authority function with federated operations. There is a growing belief that a standalone national cybersecurity agency, if appropriately structured, can substantially increase the readiness of a country's cybersecurity ecosystem. Additionally, the amalgamation of core national level functions for cybersecurity coordination, standards setting, incident response, partnership and international outreach into a centralized agency, allows governments to prioritize their limited resources.[29]

It is critical for such central agencies and other sector-level functions involved in cybersecurity to understand the threat landscape, implement appropriate defence mechanisms to protect the city from hackers, implement security controls to protect personal information from cyber criminals, maintain data privacy, and leverage safety and security in the design of a smart city.

In the following section, we provide a detailed view of the key domains that need to be considered while establishing a cybersecurity program within a smart city ecosystem.

28. EY – How to build the digital state

29. Microsoft – Building an effective national cybersecurity agency

Domain #1

Protecting smart city infrastructure from hackers

Cities are becoming smarter and improving their decision-making abilities by increasingly leveraging data from ICT systems, sensors, devices and other connected assets. However, governments need to rethink their strategies and place cybersecurity at the heart, as the proliferation of such devices creates a number of access points for cyber attackers and continues to threaten the smart city landscape. To prevent hackers from gaining unauthorized access to smart city infrastructure and systems, cybersecurity needs to be looked at from a wider lens.

Recommendation for government

As social incubators, governments should understand the complex integration of the infrastructure, transport systems, utility networks, land usage, and population demographics to better define the role they need to play in driving transformation and collaboration. The presence of a centralized cybersecurity agency at the city level has largely mitigated this challenge, and built an environment where ideas can be conceived, discussed and implemented through city-level cooperation. A holistic approach to cybersecurity has been shared based on our experience, and teaming with WGS helped better understand the business drivers for security and compliance in smart cities across the world.

Domain #2

Establishing a fit-for-purpose and risk-based security strategy

There is a growing consensus that governments often fail to embed cybersecurity throughout the processes, from strategy to design. This is mainly due to the hierarchical and bureaucratic silos, and the lack of defined roles for sector-level functions and governmental agencies. Establishing a fit-for-purpose cybersecurity strategy will assist cities in providing strategic direction to the various functions involved in ensuring cybersecurity and driving the overall security program through a rigorous, structured decision-making process.

Recommendation for government

Governments should establish the core strategic pillars for cybersecurity that will enable them to deliver the intended outcome and build an associated roadmap for enhancing the security posture. The strategy and roadmap should consider the needs of the sectors, and critical infrastructure protection should be placed in high priority. Additionally, the strategy should be risk-based and proportionate to enable sectors to innovate and implement disruptive technologies without compromising the security of the existing infrastructure.

Domain #3

Developing and implementing formalized policies, guidelines and standards at a city level

Formalized set of security policies, standards and guidelines are an essential requirement as this documents a consistent process to be undertaken by all sectorial authorities. It provides an avenue for embedding security across all critical operations and is paramount to the security of smart services being offered by governments.

Recommendation for government

Governments should define guidelines at a city level and enforce these through a centralized cybersecurity agency. While enforcing policies, governments should understand the specific risks or activities within the sectors, and therefore allow the sectoral entities to customize and/or add specific control requirements within the policies and standards, pertaining to the nature of the threats applicable (i.e., derived from a threat modeling exercise) and cater for specific technical aspects.

Domain #4

Defining a contextualized security architecture that is aligned to the needs of all relevant stakeholders

A well-defined security architecture can be used to manage the information security solutions and technologies that promote interoperability and manageability, while meeting the smart city's risk management needs.

Recommendation for government

Governments should define a security architecture that includes: an architectural description; the placement of security functionality (including security controls); security-related information for external interfaces; information being exchanged across the interfaces; protection mechanisms associated with each interface; and embedding cybersecurity in all technology implementations and projects being undertaken at a city or sector level.

Domain #5

Undertaking a holistic approach for asset management and maintaining centralized asset inventories

Smart cities utilize a wide variety of assets within critical infrastructures, which includes OT or IoT. Managing the assets is a challenge that needs to be addressed at the initial building stage of any smart city.

Recommendation for government

To address this challenge, governments should encourage sectors to maintain a single, centralized asset inventory and automate the update of the asset inventory (where feasible). This will assist smart cities in tracking and analyzing issues, such as physical location, maintenance requirements, depreciation, performance, and eventual disposal of the asset. It is to be noted that assets in an OT or IoT environment (e.g., sensors, actuators, detectors) may need a more tailored approach than generic IT assets. The assets within the inventory should be classified and governments should invest a significant amount of time in identifying crown jewel assets for prioritizing safeguards and protection mechanisms.

Domain #6

Adopting a comprehensive approach to user access control and privileged access management

Organizations that serve as critical infrastructure have interconnected corporate IT systems with production and OT environments that were traditionally segregated. Connecting ICS, SCADA and other OT systems to corporate networks has introduced known risks from the IT environment into the OT environment — including the exposure of privileged access points. These access points act as a gateway to a city's most sensitive production systems, which control the production and delivery of electricity, water, gas and other critical services to the public.

Recommendation for government

Governments should consider using privileged identity management (PIM) solutions for critical infrastructure protection (CIP) offered by various vendors to manage privileged access for critical infrastructures. In line with ISO/IEC 27002:2013, privileged access rights should be allocated to users on a need-to-use and an event-by-event basis in line with the access control policy. Additionally, the allocation of privileged access rights to systems used to operate critical infrastructures should be controlled through a formal authorization process in accordance with the relevant access control policy.

Domain #7

Managing third-party relationships using a risk-based approach

The approach of the National Institute of Standards and Technology (NIST) toward cyber supply chain risk management (C-SCRM) recommends organizations to establish an integrated third-party cyber risk assessment program that exhibits close collaboration across functional units, departments and sectors.

Recommendation for government

As it is not practical to look at every third-party relationship in minute detail, cities must establish a centralized mechanism for third-party cyber risk management based on a risk-based approach. The high-risk relationships should be managed at a central city level, whereas the lower risk relationships may be managed by the specific functions established at a sector level.

Domain #8

Enhancing security awareness using an integrated approach that involves the public and private sectors

Cyber criminals oftentimes gain access to critical infrastructure systems by targeting employees working in these areas. Additionally, residents are frequently targeted and compelled to disclose personal information on the pretext of governmental-use by impersonators. Therefore, smart cities need to build a human firewall that is aware of cyber threats through continuous and rigorous awareness and training programs.

Recommendation for government

Governments need to focus on bringing together different strengths, ideas and resources across all sectors. We recommend smart cities adopting an approach similar to the one implemented in Singapore, whereby Infocomm Development Authority of Singapore (IDA) and like-minded partners from the public and private sectors, formed the Cyber Security Awareness Alliance in 2008. Adopting this model will allow smart cities to ensure that the needs of all sectors are taken into consideration, and the awareness program covers any specific threats or topics impacting the city. Establishing awareness campaigns through these alliances, supplemented by resident groups and representatives, will assist in obtaining resident "buy-in" for the program, as the residents will feel more confident about the work being undertaken, and will actively participate in awareness campaigns.

Domain #9

Performing decentralized risk assessments while harmonizing identified risks at a city level)

Cyber risk assessments are a critical element of any business operation. They reveal sensitive areas of operations that are prone to risks and identify the associated level of security controls. The risk assessments assist in identifying areas of improvement and security controls that need to be enhanced.

Recommendation for government

Smart cities must perform periodic cyber risk assessments for target environments (e.g., critical business environments, applications, and supporting technical infrastructure). However, it is important to note that relying on public and private sectors to do their own risk assessment comes with a few disadvantages, such as lack of a harmonized approach. Smart cities could learn from practices adopted by other nation states in order to strike a balance between a centralized and federated approach to risk assessment. For example, in Switzerland, the Swiss Office of Civil Protection designed a toolkit to go alongside the national strategy for Switzerland's protection against cyber risks to overcome this challenge and drive the risk assessment in a single direction. As such, smart cities could consider establishing a risk assessment framework that mandates the structure and design of risk assessment programs across all sectors, private institutions and departments. While we anticipate that the risk assessment shall be mandated and performed on a predefined frequency, it would be of utmost importance for a central body at the city level to harmonize the risks, and advise on further actions to be undertaken. Such action would be based on a detailed study, and correlated analysis of risk details gathered and collected from various sectors.

Performing incident response on a 24x7 basis by establishing security operations center at a sectoral and city level

It is essential for a smart city to have a dedicated computer emergency response team (CERT) or a computer security incident response team (CSIRT) of its own, to decrease reliance on a national level CERT or CSIRT, which may ultimately result in timely responses to incidents encountered by the city.

Recommendation for government

In an ideal scenario, provided the cities have significant budgets, each smart city sector must consider establishing a CERT or CSIRT of its own. The advantage of having a CERT at a sector level provides a tailored and appropriate response to an incident or breach due to its ability to leverage sector-specific and operational expertise. This again eliminates the over reliance on a city-wide CERT and ensures that the city-wide CERT can focus on major incidents above a certain threshold (defined in coordination and collaboration with other sectors and governmental entities). Smart cities should also mandate incidents to be reported by third parties and service providers of critical infrastructures in a timely manner. For example, the Spanish Government, through their Royal Decree-Law mandates operators of essential services (e.g., critical infrastructures) and digital service providers to notify, on a timely basis, the incidents they suffer in the networks and information services.

Domain #11

Implementing capabilities for performing digital forensics and eDiscovery

In the current threat landscape, it is only a matter of time before a cyber criminal gains access to the infrastructure and steals confidential information, uploads malicious files or takes control of critical systems for the purpose of demanding a ransom. In such a scenario, governments would need to undertake digital forensic investigations and perform evidence handling processes to submit to lawmakers.

Recommendation for government

A vast majority of top-ranking countries within the National Cyber Security Index (NCSI), such as Greece and Estonia, have established a dedicated digital forensics unit. Establishing this unit enables smart cities to identify stealth attacks or breaches, gather evidence for known incidents, and obtain data to analyze and determine the source, attack method, objective, and impact of a particular incident. The digital forensics unit must be backed by forensic labs and digital forensic toolkits that assist in performing forensic activities in a timely and precise manner.

Domain #12

Protecting personal data by adopting a Privacy by Design approach

Privacy is considered a basic human right and is protected by national laws in different ways. Although, certain information is extremely useful for analytical institutions and governmental entities — offering best of breed services — the monetization of such data creates privacy issues. Regulators are realizing the importance of data privacy and are implementing and enforcing several data privacy, and protection requirements, however, smart cities are currently facing challenges with regard to personal data collection, disclosure, and consent management. This is mainly due to a lack of defined processes and general understanding of regulatory requirements leading to compliance complexities.

Recommendation for government

Governments need to store data within secure IT infrastructures that significantly decreases the likelihood of a privacy breach, restrict collection of personal information to a bare minimum and retain data for the shortest time possible. Dedicated tracing applications and the privacy implications that mass surveillance and monitoring has brought are key considerations within a privacy program, and should not be overlooked. Recent findings from the EY Global Consumer Privacy Survey 2020[30] found that the pandemic makes consumers more willing to share personal data for the benefit of the greater good. However, trust is still a significant issue. Almost half (47%) of consumers globally don't trust their governments to use their data beyond its stated purpose. To mitigate the challenges with respect to privacy and protection of personal information, we recommend adopting a "Privacy by Design" approach which embeds privacy into any new system, product or device throughout its lifecycle, from design to implementation. Additionally, at a smart city level, it is essential that a Data Privacy Office (DPO) is established to manage the overall data privacy and protection program.

30. EY — EY Global Consumer Privacy Survey 2020

Secure infrastructure

The goal of governments should be to build a reliable and secure infrastructure that has sufficient security controls and processes to safeguard the smart city assets.

Infrastructure housing the interconnected devices and systems forms the basis of any digital transformation journey. The infrastructure must be continually improved, in line with new technologies being adopted and implemented.

Interviewee's perspective

What are the key measures to be undertaken in order to protect residents' personal information?

Mesfer Almesfer

Chief Information Security Officer (CISO) for a cognitive smart city being developed in the Middle East region

1. Create a Data Protection Act:
   Smart cities need to have a data protection association that consults with a legal professional or an IT security expert to form an official document that clearly states the principles of how and why information can be acquired and retained.

2. Safeguard physical and electronic data:
   Smart cities must employ measures to safeguard physical and electronic data from theft or misuse. If the data is stored offline or in a physical location, lock all doors and cabinets, set up surveillance, and secure vulnerable portable devices to permanent fixtures.

3. Obtain explicit consent in forms:
   Data protection laws should mandate that consent is obtained prior to recording of any personal data. Smart cities need to utilize consent forms that allow the acquiring of consent from the individual whose data is being collected.

10

Conclusion

Rapid urbanization and increasing demands of residents are causing significant impact to city infrastructures. Cities are increasingly relying on technology and innovative services to deliver desired outcomes to residents, and enhance the ability of the workforce to provide a safe and secure environment. However, actors with malicious intent are growing in number, and seem to use sophisticated techniques to hack into critical systems and negatively impact a city's infrastructure. In the wake of this, we encourage governments to adopt a multilayered approach for responding to cyber attacks, repelling the most common attacks, with a nuanced approach for advanced and emerging threat vectors.

To protect critical information, a smart city must not only address the security of the traditional IT and OT environments, it must also deal with the added complexities from the IoTs, while also integrating innovative digital business process disruptors, such as robotic process automation (RPA), blockchain and AI. The proliferation of new connected devices and innovative ideas such as connected and flying cars, green hydrogen and cloud seeding require a Security by Design approach, as such technologies are unprecedented, and security requirements associated with them are not yet identified.

Smart cities need an enhanced approach to manage cyber attacks and remain resilient in the face of an ever-evolving cyber threat landscape.[31]

31. EY – Cybersecurity regained: preparing to face cyber attacks [Global Information Security Survey 2017–18]

Cyber attack methods

Common attacks

Defending against common attack methods means implementing solutions such as antivirus software, intruder detection and protection systems (IDS and IPS), consistent change and patch management processes, and encryption technologies to protect the integrity of data, even if an attacker does gain access to it. For a smart city, it is also essential to embed resident awareness regarding cybersecurity as they might be exposed to an attack surface (e.g., mobile applications) that will be frequently targeted by attackers.

Advanced attacks

Defending against advanced attacks requires establishments such as security operations centers (SOCs) and network operations centers (NOCs) that provide capabilities for coordination, collaboration and holistic monitoring of critical infrastructure operations. The recent trend observed for government-level SOCs has seen them adopt an active defense program, whereby multiple critical infrastructure companies share threat information and analysis on a near real-time basis, to receive and respond to security alerts and events in a coordinated manner.

Emerging attacks

Defending against emerging attacks, such as the rise in cyber-physical threats, means recognizing that some threats will be unknown. In this context, smart city authorities and governments worldwide need to create agile governance frameworks within their cybersecurity programs to ensure emerging attacks can be mitigated, and responded to in a timely and efficient manner. Smart cities with agile governance processes underlining their operational cybersecurity program are able to practice Security by Design, implementing systems and processes that are able to respond to unexpected risks and emerging dangers. Furthermore, the use of deception technology (e.g., honeypots) and bug-bounty programs (i.e., programs that encourage ethical hackers and security researchers to identify vulnerabilities in critical infrastructure systems) has significant benefits, and should be embedded within the overall program.

Governments and municipalities across the world are also struggling to tackle COVID-19 email scam campaigns that are evading traditional email security technologies.[32] Heightened fear over the virus makes users susceptible to such emails as they try to obtain new information with respect to the number of positive cases, goods, services, medical facilities, etc. Cybercriminals have been rampantly exploiting this prevalent environment to target naïve users and lure them into divulging confidential information (e.g., user credentials). Governments need to keep note of this existing environment, and consider a cybersecurity culture that needs to be driven across the smart city ecosystem consisting of governmental institutions, critical infrastructure, telecommunication companies, the private sector and residents, along with innovative technologies that are capable of keeping such criminals at bay.

Governments need to assess the good security practices mentioned so far, build on and conceptually enhance the suggested solutions. To aid in implementation and governance of smart city projects across all sectors, the government can enter into PPPs, to leverage expertise of the private sector. Government can also regularly interact with resident groups to understand their requirements, and identify improved ways of providing smart and innovative services solving a certain problem area or enhancing the existing lifestyle. Additionally, collaboration with sectoral committees, resident groups, telecommunication companies, industry forums, threat intelligence sharing entities, backed by agile governance frameworks will be a key enabler to tackling cybersecurity risks and issues in the long run.

32. EY – Seven ways to keep ahead of COVID-19 cyber attackers

About the partner and coauthors

Partner

Samer Omar

Principal, EY Consulting LLC, Dubai
Email: samer.m.omar@ae.ey.com

Coauthors

Ritesh Guttoo

Partner, EY Africa Cybersecurity Leader
Ernst & Young Ltd, Mauritius
Email: ritesh.guttoo1@mu.ey.com

Siddhesh Mudbhatkal

Manager, Technology Consulting
Ernst & Young Ltd, Mauritius
Email: siddhesh.mudbhatkal@mu.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

The MENA practice of EY has been operating in the region since 1923. For over 97 years, we have grown to over 7,500 people united across 21 offices and 16 countries, sharing the same values and an unwavering commitment to quality. As an organization, we continue to develop outstanding leaders who deliver exceptional services to our clients and who contribute to our communities. We are proud of our accomplishments over the years, reaffirming our position as the largest and most established professional services organization in the region.

EYG no. 006954-21Gbl

ED None

ey.com