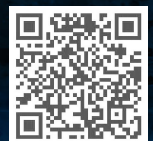




Making smart cities cybersecure

Ways to address distinct risks in an increasingly
connected urban future



#SalmanQadir

About the authors

PIYUSH PANDEY is the managing director of Deloitte's Risk and Financial Advisory practice and Smart Cities Cybersecurity leader. He has more than 17 years of experience, including enabling digital transformation of state, local, and city governments by shaping cybersecurity vision and strategy; design and implementation of identity solutions and advanced authentication programs; development of security standards and solutions, as well as resiliency and incident management plans; implementation of vulnerability management solutions; and establishment of data protection and privacy programs. Pandey has an undergraduate degree in computer science and a master's in business administration.

DEBORAH GOLDEN is a Deloitte Risk and Financial Advisory principal and leads cyber risk services for the Government & Public Services (GPS) practice of Deloitte & Touche LLP. She is also the GPS empowered well-being leader and the lead principal for a major federal government health care provider. She has almost 25 years of information technology, security, and privacy experience spanning numerous industries, including a specialization in cybersecurity and technology transformation. Golden has also coauthored reports on cybersecurity, including *AI-augmented cybersecurity* and *Addressing cyber threats: Multi-factor authentication for privileged user accounts*.

SEAN PEASLEY is a Deloitte Risk and Financial Advisory partner and the Consumer & Industrial Products leader and Internet of Things (IoT) security leader in Cyber Risk Services at Deloitte & Touche LLP. He has more than 32 years of experience helping organizations address their most pressing and pervasive cyber risk challenges. His areas of focus include cyber risk management, cyber threat intelligence, cyber war-gaming, identity and access management, IoT security, privacy and data protection, and business. He has experience in several industries, including automotive, consumer products, health care, industrial products and services, manufacturing, and retail.

MAHESH KELKAR, Deloitte Services LP, is a research manager with the Deloitte Center for Government Insights. He closely tracks developments in the federal and state government sectors, and focuses on conducting in-depth research on the intersection of technology with government operations, policy, and decision-making.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Contents

Introduction		2
Smart cities face unique cyber risks		3
Convergence of the cyber and physical worlds		5
Interoperability between legacy and new systems		6
Integration of disparate city services and infrastructure		7
A holistic approach to cybersecurity		9
Securing cities for growth		12
Endnotes		14

Introduction

SMART CITIES ARE the future of urban living, harnessing the power of three Ds—digital technologies, data, and design thinking—to boost the efficiency and effectiveness of city services. However, this new wave of digital transformation also brings new cyber risks that could fundamentally impact the existence of smart cities. Cyber threats have been on the rise for years, but the last few years have seen an explosion in cyberattacks that target both data and physical assets.¹

As connected devices proliferate at a breakneck speed—the number of IoT devices is expected to rise from 8.4 billion today to almost 20 billion by 2020²—cyberattacks and vulnerabilities in one area can have a cascading effect on numerous other areas. The consequences could extend beyond just data loss, financial impact, and reputational damage

risks—severe enough as they are—to include disruption of crucial city services and infrastructure across a broad range of domains such as health care, transportation, law enforcement, power and utilities, and residential services. Such disruptions can potentially lead to loss of life and breakdown of social and economic systems.

The rapid hyperconnectivity and digitization of cities are accelerating cyber threats. To tackle the challenge, government leaders, urban planners, and other key stakeholders should make cybersecurity principles an integral part of the smart city governance, design, and operations, not just an afterthought. In this paper, we examine the key factors that influence cyber risks in a smart city ecosystem and a broad approach that city leaders can adopt to manage these risks.

In March 2018, the city of Atlanta faced a ransomware attack that hit some of its customer-facing applications.³ At one point, the city had to shut down its free Wi-Fi network at the Hartsfield-Jackson Airport as a precautionary measure. Overall, the attack hit 5 out of 13 city departments, and it took the city weeks to get back to normalcy.⁴ Such attacks are also growing in frequency: According to a 2016 survey of chief information officers of cities and counties, about a quarter of local governments were facing attempted cyberattacks every hour.⁵



Smart cities face unique cyber risks

A SMART CITY IS a complex ecosystem of municipal services, public and private entities, people, processes, devices, and city infrastructure that constantly interact with each other. The underlying technology infrastructure of the ecosystem comprises three layers: the edge, the core, and the communication channel (figure 1). The edge layer comprises devices such as sensors, actuators, other IoT devices, and smartphones. The core is the technology platform that processes and makes sense of the data flowing from the edge. The communication channel establishes a constant, two-way data exchange between the core and the edge to seamlessly integrate the various components of the ecosystem.

This massive amount of data exchanges, integration between disparate IoT devices, and dynamically changing processes creates new cyber threats, compounded by complexities in the other components of the ecosystem that wrap around the technology infrastructure. For instance, data governance can be a thorny issue for cities as they need to think about whether the data is internal or external; whether it is transactional or personalized; whether the transactional data is collected via IoT devices; and how the data is stored, archived, duplicated, and destroyed. In addition, due to a lack of common standards and policies, many cities are experimenting with new vendors and products, which create interoperability and integration problems on the ground and exacerbate cyber risks.

FIGURE 1

The smart city ecosystem comprises three layers: The edge, the core, and the communication channel

THE CORE

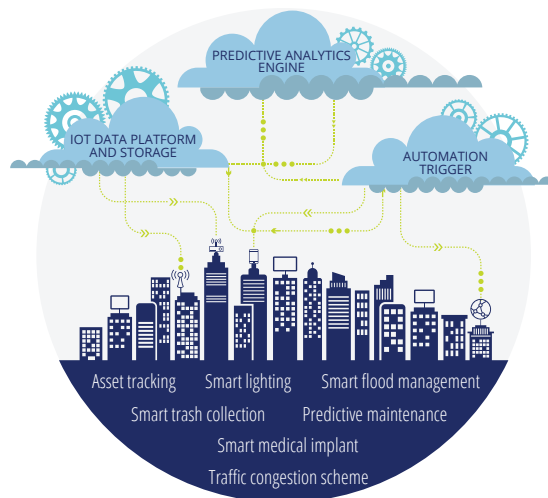
The core is the technology platform (cloud platform, IoT data platform) that processes data and generates business logic to make sense of the data flowing from the edge.

THE COMMUNICATION LAYER

The communication channel (Bluetooth, NFC, LTE, WiFi Direct, etc.) establishes a constant, two-way data exchange between the core and the edge to seamlessly integrate the various components of the ecosystem.

THE EDGE

The edge layer comprises devices such as sensors, actuators, and smart phones, as well as IoT applications such as smart lighting and smart trash collection. This is the front end of the smart city.



Source: Deloitte analysis.

Three factors influence the potential cyber risk in a smart city ecosystem (figure 2):

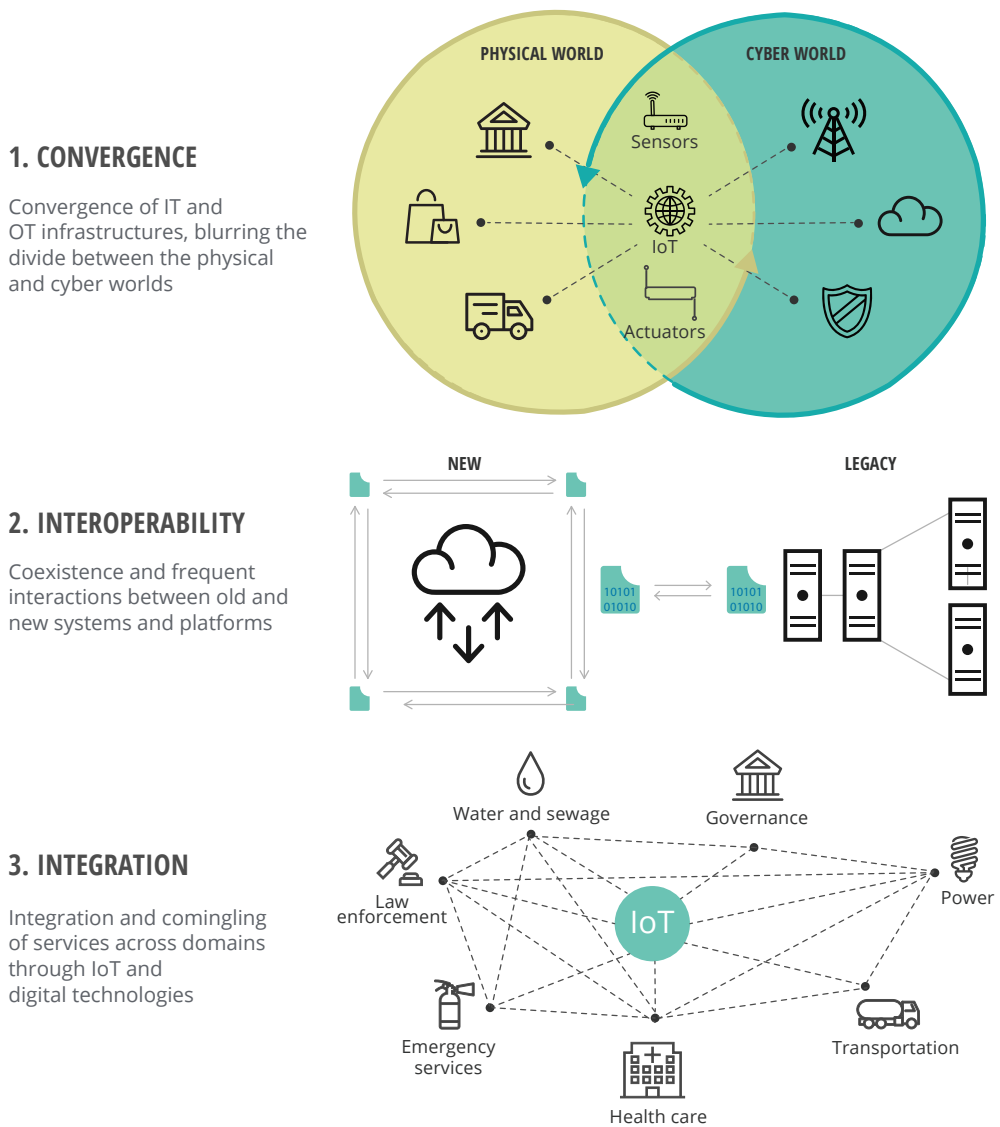
1. Convergence of the cyber and physical worlds
2. Interoperability between legacy and new systems

3. Integration of disparate city services and enabling infrastructure

To begin to understand how to manage the cyber risk landscape, it helps to explore each of these factors further.

FIGURE 2

Three key factors influence cyber risk in cities



Source: Deloitte analysis.

Convergence of the cyber and physical worlds

SMART CITIES BLUR the lines between the physical and cyber worlds. In this environment, people, processes, and places are integrated via both information technology (IT) systems used for data-centric computing and operational technology (OT) systems used to monitor events, processes, and devices and adjust city operations. Such convergence allows cities to control and govern technology systems through remote cyber operations.

However, this convergence, where many devices in the edge could be cyber threat vectors, gives rise to the risk of malicious actors entering the system and disrupting operations on the ground—thus

Convergence of IT and OT allows cities to control and govern technology systems through remote cyber operations—but also exponentially expands the cyber risk landscape.

exponentially expanding the cyber risk landscape.⁶ With the proliferation of IoT devices, attackers now have countless entry points to compromise a city's systems and take advantage of the resulting vulnerabilities.

In 2014, a German steel mill was a victim of a spear phishing attack. Through targeted emails appearing to be from a trusted source with a malicious attachment, the attackers first obtained access to the business network and then to the production network lacking required separation. The attackers remotely disabled the blast furnace by taking over the control systems, resulting in massive physical damage to the furnace system, costing millions of dollars.⁷

In another example, as an experiment, University of Michigan researchers successfully targeted the Intelligent Traffic Signal System (I-SIG), which is one of a series of CV-based transportation systems being deployed, tested, and implemented under the US Department of Transportation's CV Pilot Deployment Program. The researchers used data spoofing and fake messages from a nearby connected vehicle to create a traffic jam in a simulated environment, increasing average delays by 38 percent.⁸ This attack turned out to be quite easy to do, highlighting the expanding cyber risk landscape.

Interoperability between legacy and new systems

OFTEN, ORGANIZATIONS THAT pursue digital transformation need to integrate new digital technologies with legacy systems, which can create significant challenges and risks. These challenges include inconsistent security policies and procedures and disparate technology platforms, resulting in hidden security vulnerabilities throughout the smart city ecosystem.

Disparate technology platforms can result in hidden security vulnerabilities throughout the smart city ecosystem.



This situation is exacerbated as many cities increasingly use IoT solutions, but within a retrofitting model. For instance, large, established gas and water systems within a city have deployed sensors on a large scale. These sensors need to connect to a broader network for the data to be aggregated and analyzed centrally. However, these sensors have minimal security protocols.⁹ In the long run, retrofitting may not be a viable option as many devices could become physically incapable of upgrades.¹⁰

Another challenge is the lack of generally accepted standards governing the functioning of IoT-enabled devices. City departments and agencies typically use sensor technologies from different vendors that generate data in different formats and use different communication protocols. Creating interoperability in such situations can be difficult, and cities may face a trade-off between interoperability and security. Each new device added to an IoT ecosystem adds a new attack surface or opportunity for malicious attack.¹¹

In 2015, the US Office of Personnel Management's (OPM's) systems suffered a data breach, giving hackers access to personnel file records of 4.2 million employees. This breach was primarily due to the OPM's old network's inability to encrypt data.¹² The OPM has spent millions of dollars since then to accelerate the modernization process.¹³

Integration of disparate city services and infrastructure

TRADITIONALLY, CITIES HAVE offered a wide range of services that were largely independent of each other (e.g., power, water, sewer, transportation, public works, law enforcement, firefighting, and social services). Each of these services was typically provided by an agency using its own systems, processes, and assets. Now, these services are slowly being integrated and linked through an interconnected web of digital technologies.

As cities gain opportunities for new services and efficiencies, this comingling of services and systems comes with its own set of challenges. The increasing integration, interconnectedness, and data exchange create shared vulnerabilities where a problem in one service area can quickly cascade into other areas—potentially leading to widespread and catastrophic failures. In addition, cities need to rethink regulatory requirements, rationalize varied security protocols, and address data ownership and usage challenges.

A problem in one service area can quickly cascade into other areas—potentially leading to widespread and catastrophic failures.

Furthermore, data stored in different systems can be susceptible to misuse, potentially affecting citizens' privacy. For instance, it is a leading practice to mask or delete personal identifiers in data. However, techniques and methods that allow malicious attackers to match different datasets to reidentify an individual are becoming increasingly sophisticated. So, a breach that compromises multiple systems and datasets can become a serious privacy incident for cities.

Cyber risk will continue to evolve in the coming years, as many cities plan to integrate a wide variety of services and infrastructure, connecting even more data, systems, and devices.

The Emotet malware virus struck the city of Allentown, Pennsylvania, in February 2018. The virus quickly multiplied in a week and rendered the city's finance department system unusable by not allowing it to make external bank transactions. Also, the police department could not access databases controlled by the Pennsylvania state police. Containing the virus and getting back to operational status is estimated to have cost the city US\$1 million.¹⁴

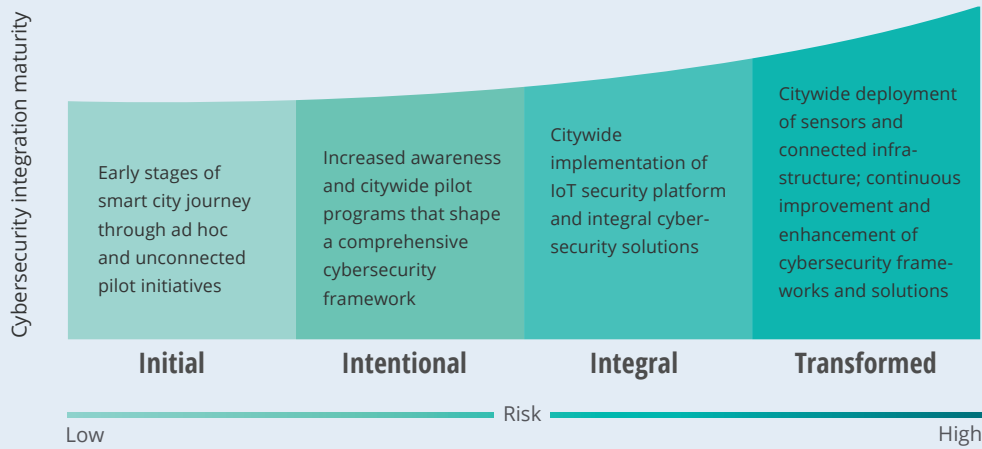


UNDERSTANDING THE CYBER RISK EVOLUTIONARY CURVE IN SMART CITIES

Most smart cities follow a four-stage evolutionary path that relies on varying mixes of new and legacy technologies. With each step up the curve, the scale of technology infrastructure and the potential attack vectors can significantly increase, necessitating corresponding maturity in the cybersecurity strategy (figure 3).

FIGURE 3

Cybersecurity strategies need to evolve along with smart cities' digital transformation



Source: Deloitte analysis.

During the initial stage, when data is being collected through a small number of city-controlled, hard-wired sensors, the potential breach points are generally limited. However, at the next (intentional) stage, when a city starts to collect data from citizens' smartphones and connected infrastructure, there are suddenly millions of uncontrolled potential breach points, most of which are beyond the city's control. In the most advanced stages, when software bots at the core use artificial intelligence to make decisions and act without human involvement, the potential attack vectors are nearly endless—and continuous.

It is important to note that as a city moves up the evolutionary curve, the degree of convergence, scale of technology infrastructure and corresponding interoperability, and integration of services increase. For instance, while a city might have a few hundred connected devices in the initial or intentional stage, the same number can be in thousands or millions in the integral and transformed stages and will require better infrastructure to support such growth. The situation, in turn, drives more complexity in the core, edge, and communication layers of the smart city ecosystem. Therefore, the maturity of cyber risk capabilities should be directly proportional to the degree of integration of smart city ecosystem components, and the cyber risk management approach should consider all these components.

A holistic approach to cybersecurity

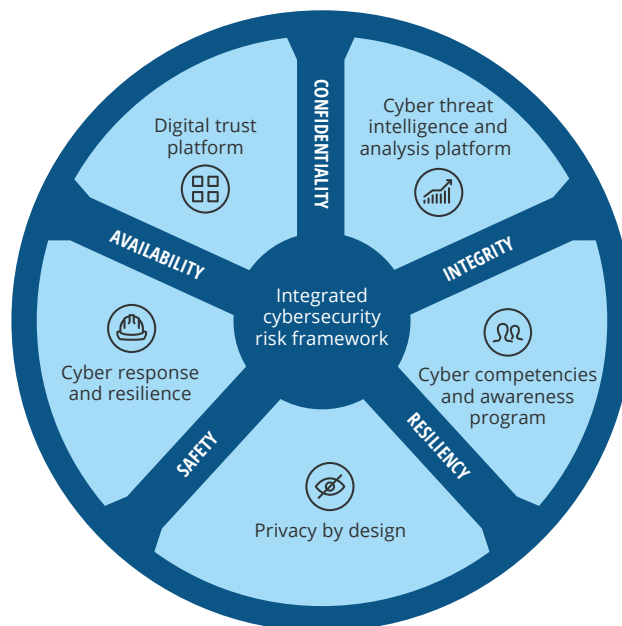
THE CONVERGENCE OF physical and digital infrastructure, the ensuing interoperability, and interconnectedness between city systems and data is an ongoing effort in many cities. The security goals of a smart city—**confidentiality, integrity, availability, safety, and resiliency**—should be grounded on both the objectives of traditional IT (to secure data) as well as those of OT (to ensure safety and resiliency of systems and processes). These combined security objectives can help cities maintain a more secure and resilient operating environment (figure 4).

An integrated cyber risk framework can provide cities with management principles to incorporate

into their smart city planning, design, and transformation stages. It comprises industry standards, legal, and regulatory requirements to determine how cyber risk may affect all the ecosystem participants, including users, government, services, infrastructure, and processes, as well as assess each system’s and asset’s influence on each other. Such an integrated approach can enable city stakeholders to view threats and vulnerabilities in their entirety rather than react to specific services or operational impact, eventually allowing them to develop the core capabilities of a cybersecurity program described in figure 5.

FIGURE 4

Smart cities must take a holistic approach to smart city cybersecurity




Source: Deloitte analysis.

FIGURE 5

An integrated approach to cybersecurity is based on five core components

Component	Details	Examples and context
 <p>Digital trust platform</p>	<p>A platform that enables seamless trusted connections and manages identities and relationships within a connected ecosystem. It can help manage the contextual relationships between people, devices, and systems. The approach should be designed to enable cities to identify, authenticate, and authorize people and devices through an adaptive, behavior-based security mechanism, augmented by geospatial technologies to provide location-based situational awareness.</p>	<p>Recent advancements in microprocessors enable low-powered hardware products that embed security features—such as providing trusted identities to certify devices on networks—directly into IoT devices. Previously, most IoT device manufacturers offered external security to the devices at the software and cloud levels, but now manufacturers can extend that to the device controller level.¹⁵ Meanwhile, advances in blockchain technology can offer a secure, self-sovereign identity that could enable efficient transactions across a wide variety of asset classes.¹⁶</p>
 <p>Privacy-by-design</p>	<p>Privacy-by-design is a concept that aims to protect citizens' privacy by incorporating it upfront in the design of technologies, processes, and infrastructure. It can help restrict the collection of personal data, enable stricter data encryption processes, anonymize personal data, and address data expiry. Privacy setting notices can be designed in a user-friendly way.</p>	<p>Imagine a system where citizens can own their data and also control access to that data. For instance, citizens can have full control of their medical records data and can provide access to specific doctors of their choosing. Additionally, medical professionals can only see the data and not store it; hence when a citizen decides to revoke access, others no longer have access to the record. For instance, Estonia's X-Road data-exchange system has privacy built into the system.¹⁷</p>
 <p>Cyberthreat intelligence and analysis platform</p>	<p>An ecosystemwide platform with reconnaissance capabilities that enable cities to look beyond internal data and identify threat based on active events and external databases. By using behavioral analytics, machine learning, and artificial intelligence capabilities, the platform can provide a complete picture of the threat landscape to better inform scenario planning and response.</p>	<p>The city of Los Angeles' (LA) integrated strategic operations center (ISOC) processes cyber threat information and monitors threats to prevent them from becoming incidents. The ISOC is an important link in the city's vigilance against cyber threats. It processes threat information from the Department of Homeland Security, the FBI, the private sector, and other nonprofit sources and passes it on to city departments and other important entities such as the Port of LA and LA International Airport.¹⁸</p>
 <p>Cyber response and resilience</p>	<p>Cyber response and resilience is about being prepared for a potential cyberattack. To help stay prepared, cyber war-gaming or simulations can help city governments gauge their speed and readiness to respond to cyber threats and create a stronger resiliency plan to manage potential attacks.¹⁹ This also includes developing advanced cyber forensic capabilities to help trace a threat and contain it, preventing it from spreading to other city systems.</p>	<p>In the IoT era, cyber resilience should be in the form of fail-safe systems. For instance, if one of the devices in the ecosystems fails, it should not trigger a knock-out systems failure. Thus, threats need to be contained to a smaller area, avoiding larger catastrophic failure. This can be achieved by building a stronger security event-monitoring control in the system. With more effective incident or error handling at the component level, the system can shut down the affected connected device in a fail-safe manner.²⁰</p>

Component	Details	Examples and context
 <p>Cyber competencies and awareness program</p>	<p>The cyber workforce shortage continues to be a challenge for governments and can be a hurdle in driving the cybersecurity strategy in a city. According to the 2018 Deloitte-National Association of State Chief Information Officers (NASCIO) cybersecurity survey, cyber staffing and competency gaps continue to be a pain point for state chief information security officers (CISO).²¹ Smart city operations are expected to require new kinds of workers with cyber-related capabilities in many parts of the workforce, not just IT. For example, traditional urban infrastructure development generally required civil engineering expertise. However, as smart cities blur the line between physical and digital infrastructure, there is a need for civil engineers with a broad understanding across multiple physical and digital infrastructure systems including data governance and information and communication technologies that go beyond the traditional civil engineering training.</p>	<p>For more traditional cybersecurity roles and responsibilities, the National Institute of Standards and Technology (NIST) has developed a resource that categorizes and describes cybersecurity work in detail. NIST's NICE Cybersecurity Workforce Framework maps cyber skills to seven categories, 33 specialty areas, and 52 work roles.²² A city government can use this framework as a starting point to identify and communicate cyber skills shortages and devise ways to plug skills gaps.²³</p>

Source: Deloitte analysis.

Securing cities for growth

BALANCING THE PROMISE of smart cities against the potential of cyber risks—and managing the associated risks effectively—will be critical to realizing the potential of smart cities. Cities should begin by engaging all the stakeholders and entities in the broader ecosystem. The next steps that cities should consider include the following:

- **Syncing smart city and cyber strategy.**

Cities should define a detailed cybersecurity strategy that is in line with their broader smart city strategy and that can mitigate challenges arising from the ongoing convergence, interoperability, and interconnectedness of city systems and processes. Cities should consider carrying out an extensive impact assessment of their data, systems, and cyber assets to identify, assess, and mitigate the risks associated with technology processes, policies, and solutions. The integrated view of the risks and knowledge of interdependencies of the critical assets can enable cities to develop a comprehensive cybersecurity strategy. For instance, Singapore launched its National Cyber Security Master plan in 2013 and followed it with a new cyber security bill in 2016. Both initiatives were an integral part of Singapore’s smart nation strategy.²⁴

- **Formalizing cyber and data governance.**

Cities need to formalize the governance approach to data, assets, infrastructure, and other technology components. A comprehensive governance model should spell out responsibilities and roles for each critical component in the smart city ecosystem. To implement an ecosystem approach to tackling cyber issues, various entities will need to work together with a strong

governance model as the foundation. Cities can establish a network among other cities, state agencies, academia, and corporations to share threat information, capabilities, and contracts to strengthen cyber defenses.²⁵ Additionally, data management—including robust data sharing and privacy policies, data analytics skills, and monetization models that facilitate the sourcing and usage of “city data”—constitutes a critical aspect of this governance. Policies, legislation, and technology must be continuously aligned to maintain the right balance of protection, privacy, transparency, and utility. The governance, policies, and processes must mature along with the city’s overall cyber strategy. For instance, the city of Hague is home to the “Hague Security Delta,” an ecosystem of more than 200 organizations working in the national security, cyber and urban security, critical infrastructure, and forensics.²⁶

- **Build strategic partnerships to grow cyber capabilities.**

The cyber skills gap is not going away anytime soon, so cities need to be innovative and proactive in plugging the cyber skills gap in their cities. This approach may require city administration to explore nontraditional efforts to tap into cyber talent such as crowdsourcing, prizes, and challenges to solve cyber-related issues. A smart city requires new skills and competencies across the various ecosystem layers. Cities can augment existing capabilities through strategic partnerships and contracts with service providers.

It is critical for city leadership to realize that securing cities from cyber risk is not a one-time event where cyber strategy evolves as cyber threats evolve;

instead, it is also important to be able to recover when a cyberattack happens. Also, this is not a battle that cities can or should fight alone, but instead with an ecosystem of city governments, academia, the private sector, and startups. Technology can be one part of the cybersecurity solution, but the latter also needs a comprehensive governance model toward

data and assets. More importantly, cities need an integrated approach to managing cyber risk with cybersecurity principles baked into every stage of the smart city development process (i.e., from strategy and design to implementation and operations). Cybersecurity is just too important to be treated as an afterthought.



Endnotes

1. World Economic Forum, *The global risks report 2018*, 2018.
2. John P. Dzrik, "Cyber risk is a growing challenge. So how can we prepare?," World Economic Forum, January 17, 2018.
3. Jerry Bowles, "America's cities are under cyberattack. That's bad news for IoT and Smart Cities," Diginomica, March 30, 2018.
4. Mary Scott Nabers, "Smart city security: Atlanta cyberattack cripples city," IoT Word Today, April 5, 2018.
5. ICMA, *Cybersecurity 2016 survey*, April 19, 2017.
6. Irfan Saif, Sean Peasley, and Arun Perinkolam, "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age," *Deloitte Review* 17, July 27, 2015.
7. Kim Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *Wired*, January 8, 2015.
8. Qi Alferd Chen et al., "Exposing congestion attack on emerging connected vehicle based traffic signal control," University of Michigan, February 18–21, 2018.
9. Saif, Peasley, and Perinkolam, "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age."
10. Ibid.
11. Ibid.
12. Phil Goldstein, "Legacy federal IT systems are a ticking time bomb of risks," FedTech, December 7, 2015.
13. Jason Miller, "3 years after data breach, OPM still struggling to modernize IT," *Federal News Network*, February 27, 2018.
14. Daniel Patrick Sheehan, Emily Opilo, and Daryl Nerl, "City of Allentown computer systems hit by virus that will require nearly \$1M fix," *The Morning Call*, February 20, 2018.
15. Trevor Jones, "Microsoft takes holistic approach to IoT security concerns," TechTarget, April 18, 2018.
16. Mark White, Jason Killmeyer, and Bruce Chew, *Will blockchain transform the public sector?*, Deloitte University Press, September 11, 2017.
17. William D. Eggers, *Delivering on Digital: The Innovators and Technologies That Are Transforming Government* (New York, Rosetta Books, 2016), pp. 164–5.
18. Joseph Marks, "LA cyber center hopes to be a model for cities nationwide," Nextgov, December 7, 2017.
19. Eggers, *Delivering on Digital*, pp. 199–200.
20. Saif, Peasley, and Perinkolam, "Safeguarding the Internet of Things: Being secure, vigilant, and resilient in the connected age."
21. Srini Subramanian and Doug Robinson, *2018 Deloitte-NASCIO cybersecurity study: States at risk—bold plays for change*, Deloitte Insights, October 22, 2018.
22. National Institute of Standards and Technology, "NICE cybersecurity workforce framework," accessed July 17, 2018.

23. Deborah Golden and Ted Johnson, *Augmented security*, Deloitte University Press, 2017.
24. FTI Consulting, *Singapore's approach to cyber security*, 2016.
25. Subramanian and Robinson, *2018 Deloitte-NASCIO cybersecurity study*.
26. Hague Security Delta, "About HSD," accessed on April 13, 2018.

