A Cybersecurity Guide for Smart Cities

AUTHORS: Lorenzo **Cotino**
Marco **Sánchez**

EDITORS: Mauricio **Bouskela**
Gilberto **Chona**
Ariel **Nowersztern**
Patricio **Zambrano-Barragán**
Isabelle **Zapparoli**

IDB

A Cybersecurity Guide for Smart Cities

Authors:
Lorenzo Cotino
Marco Sánchez

Editors:
Mauricio Bouskela
Gilberto Chona
Ariel Nowersztern
Patricio Zambrano-Barragán
Isabelle Zapparoli

Inter-American Development Bank

December 2021

Cataloging-in-Publication data provided by the
Inter-American Development Bank
Felipe Herrera Library

A cybersecurity guide for smart cities / Lorenzo Cotino, Marco Sánchez; editors, Maurício Bouskela, Gilberto Chona, Ariel Nowersztern, Patricio Zambrano-Barragán, Isabelle Zapparoli.
p. cm. — (IDB Monograph ; 963)
Includes bibliographic references.
1. Smart cities-Latin America. 2. City planning-Technological innovations-Latin America. 3. Computer security-Latin America. 4. Computer crimes-Latin America-Prevention. I. Cotino Hueso, Lorenzo. II. Sánchez, Marco. III. Bouskela, Maurício, editor. IV. Chona, Gilberto, editor. V. Nowersztern, Ariel, editor. VI. Zambrano-Barragán, Patricio, editor. VII. Zapparoli, Isabelle, editor. VIII. Inter-American Development Bank. Housing and Urban Development Division. IX. Inter-American Development Bank. Innovation in Citizen Services Division. X. Series.
IDB-MG-963

JEL codes: J18, K24, L86, L88, L90, L94, L95, L96, L98, M15, N96, O14, O18, O19, O31, O32, O38

Keywords: cybersecurity, cyberattacks, cyberspace, data protection, governance, asset protection, cities, smart cities, information systems, information technologies, internet of things, urban infrastructure, urban services, Latin America and the Caribbean, information security, computer security, digital transformation, CISO.

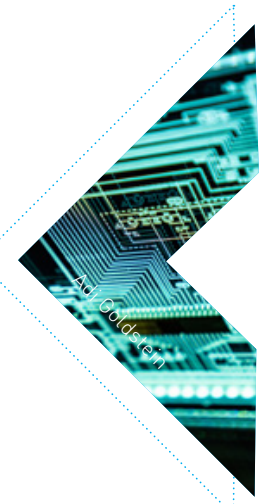
This cybersecurity guide for cities and subnational governments provides knowledge and recommendations to help the cities of Latin America and the Caribbean (LAC) to protect themselves in cyberspace. The guide is aimed at city leaders, municipal managers and employees, and IT staff. It is divided into five parts. The first part addresses the general questions of cybersecurity and the main aspects that compose it: actors, risks, and impacts. The second part includes a roadmap for beginning to address cybersecurity at the local level. The third part presents a series of recommendations aimed at three key audiences of local administration. The fourth part gives detailed information and references regarding risk management models, tools, and other instruments useful for municipal IT staff. Finally, it reviews the IDB's own contribution in this area before presenting the conclusions.

https://www.iadb.org

Translation: Richard Torrington

Revision: Dawn Hunter, Leslie C. Hunter, and Sarah Schineller

Design: Ramón Zamora



This cybersecurity guide for cities aims to provide knowledge and added value to better understand cybersecurity, risks, potential impacts, and the urgency to act proactively to protect the cities of Latin America and the Caribbean.

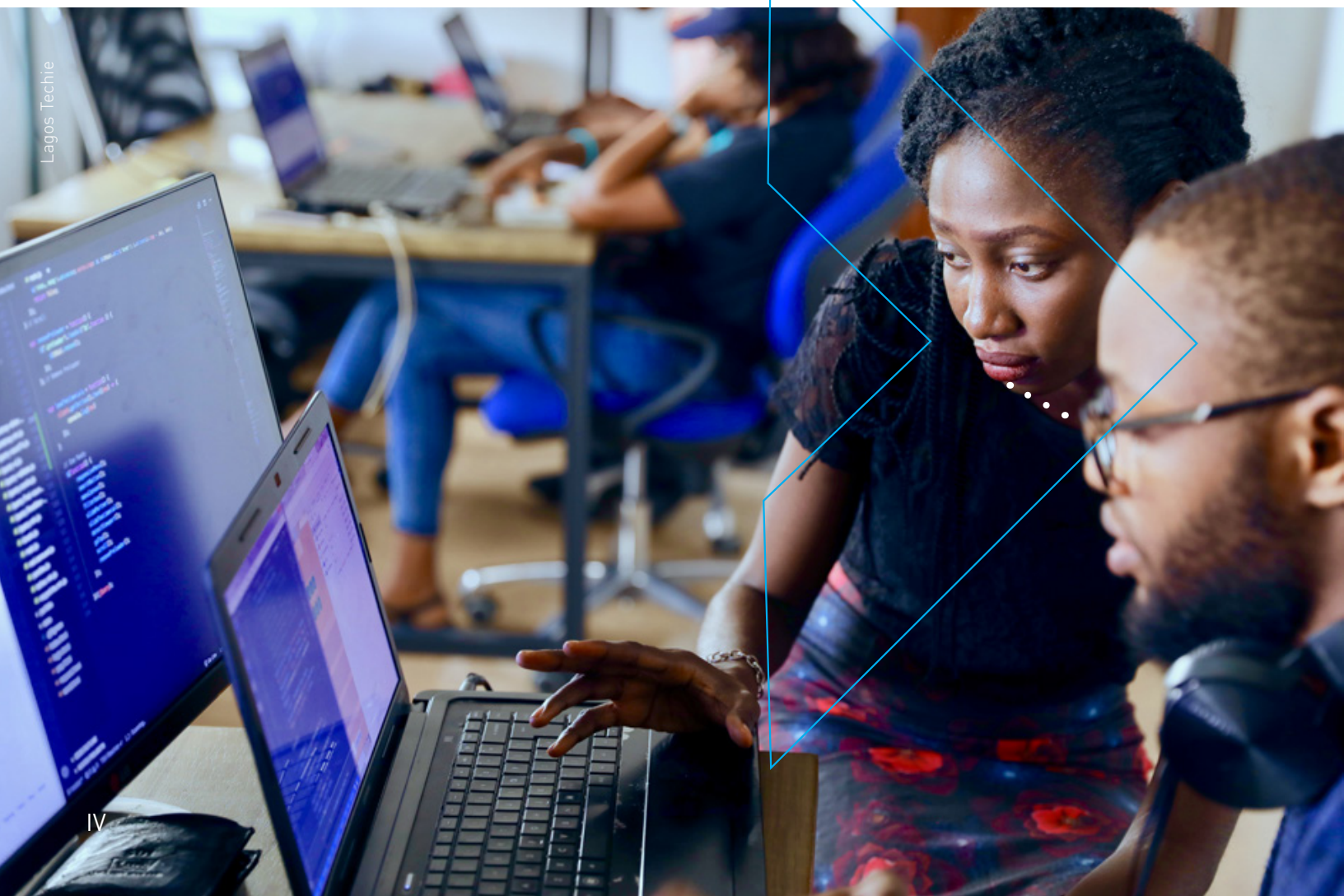

Lagos Techie

Table of Contents

Adam V

Preface

Román López

"This cybersecurity guide for cities is an early contribution to an emerging discussion that will lead us to consistent and overarching responses to the challenge of cybersecurity for the resilient, sustainable, and equitable development of our cities."

Preface

Digitalization is a central element of the Inter-American Development Bank's "Vision 2025: Reinvest in the Americas."[1] It is based on the idea that exploiting the immense potential of digital transformation to the maximum requires strategic, long-term thinking, better connectivity, more human capital, and sound digital infrastructure. It means strengthening digital governance, encouraging innovation, and updating obsolete regulations that govern information and communication technologies (ICTs).

With the advent of the COVID-19 pandemic, the process of digitalization at the global level accelerated markedly and brought with it significant changes in the way we live, work, and communicate. Digitalization increased in firms, households, and public services.

It has introduced new ways of accessing information and services, opened up new channels of communication between government and citizens, and offers opportunities to improve governance in general.

This shift in the digital paradigm affects metropolitan areas and municipalities. In fact, cities are increasingly important agents in advancing global digitalization. The adoption of new digital technologies is an essential characteristic of urban development. It drives innovation, better communication, collaboration, equality, and efficiency.

However, as local government management, infrastructure, and urban services become more digitalized, their exposure to risks and vulnerabilities from cyberattacks grows in tandem. In other words, reliance on IT to manage and monitor the essential systems that maintain key areas such as security, water, energy, mobility, and response to catastrophic climate change-related events increases the risk of cyberattacks.

1. See https://www.iadb.org/en/about-us/overview.

Cybersecurity has rapidly become a key element of sound city governance. Cyberattacks have considerable potential to disrupt the operations of cities and affect their finances and the reputation of their administrations, while inflicting significant damage on information systems for an indefinite period. Such cyberattacks threaten the continuity of services, timely access to information, the privacy of personal data, and payment by digital methods used by municipalities and citizens, among other critical areas.

Inevitably, cities will continue to be exposed to cybersecurity breaches. Although many cities have suffered cyberattacks, problems and challenges remain in governance and risk management with respect to proactively addressing cybersecurity, especially at the municipal level.

Goh Rhy Yan

The available data clearly indicate that cyberattacks and incidents, in particular those perpetrated with criminal intent, are increasing in both frequency and sophistication, and may be very costly. Furthermore, cyber crime does not stop at national borders; it is a problem that affects the entire public sector (national or subnational) and private sector organizations.

Recently, the IDB has made significant efforts to address the knowledge gaps in cybersecurity and to help national public sector agencies and private firms to improve their frameworks, measures, and capacities to strengthen cybersecurity, while emphasizing the need to deepen cooperation and improve the exchange of information.

With respect to tackling the vulnerability of cities to cyber crime, the main challenges are related to weak governance and a lack of awareness of the gravity of the risks and the potential damage from a possible cyberattack. Furthermore, inadequate resource allocation to cover multiple priorities in a context of budget cutbacks, as well as the lack of qualified human resources, exacerbates the problem.

For the region's cities, the question is not if a cyberattack is going to happen, but when. Cities can plan proactively to ensure that cyberattacks do not cause disruptions to their governance and administrative management.

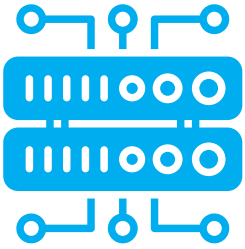
This publication explores cybersecurity in cities to promote knowledge about cyber protection and actions that the major cities of Latin America and the Caribbean (LAC) can take. Its frank and open treatment of the subject will serve as an initial guide for metropolitan decision-makers to strengthen their digitalization processes while reducing their vulnerability to cyberattacks.

Specifically, this guide will help raise awareness about the importance of urban cybersecurity frameworks and processes. Among other tools, it proposes a roadmap and a plan of action for cities in the LAC region.

This cybersecurity guide for cities is an early contribution to an emerging discussion that will lead us to consistent and overarching responses to the challenge of cybersecurity for the resilient, sustainable, and equitable development of our cities. Our goal is to improve lives in our increasingly digitalized cities, and we want to do it safely.

Tatiana Gallego Lizón
Head of the Housing and Urban Development Division
Climate Change and Sustainable Development Sector
Inter-American Development Bank

Edgardo Mosqueira Medina
Head of the Innovation in Citizen Services Division (AI)
Sector of Institutions for Development
Inter-American Development Bank



Prologue and Acknowledgments

Jurriaan

"Municipal governments are increasingly using digital technology, the internet, and mobile technology to plan, connect, and manage their infrastructure and provide urban services, to improve the quality of life of their inhabitants."

Prologue and Acknowledgments

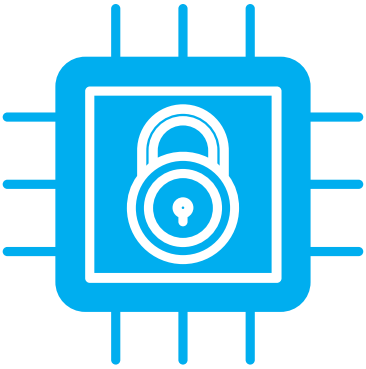
This guide emerged from the IDB's reflections on how to help the region's cities to protect themselves in cyberspace while transforming their traditional management model into an intelligent model.

Municipal governments are increasingly using digital technology, the internet, and mobile technology to plan, connect, and manage their infrastructure and provide urban services, to improve the quality of life of their inhabitants. Following the pandemic, the digitization of cities has accelerated. More connected cities, however, are also more exposed cities. The risk of becoming the target of a cyberattack is growing. The economic cost of having the city's operations paralyzed is extremely high and jeopardizes not only infrastructure and urban services but also citizen security.

The preparation of this guide involved a joint effort by the departments of Climate Change and Sustainable Development (CSD), Institutions for Development (IFD), and Knowledge, Innovation and Communication (KIC), led by Juan Pablo Bonilla, Moisés Schwartz, and Federico Basañes, respectively. The Housing and Urban Development Division (CSD/HUD) and the Innovation in Citizen Services Division (IFD/ICS) provided technical supervision under the aegis of Tatiana Gallego Lizón and Edgardo Mosqueira Medina (AI), respectively. Mauricio Bouskela, Gilberto Chona, and Ariel Nowersztern were in charge of coordination, with the support of Isabelle Zapparoli, and were responsible for editing the text, with contributions from Patricio Zambrano-Barragán and Miguel Ángel Porrúa as reviewers of content and approach.

The authors, Lorenzo Cotino Hueso (Spain) and Marco E. Sánchez Acevedo (Spain-Colombia), are university professors and legal experts in cybersecurity and the use of IT by public administrations. Working alongside them, the team coordinator selected the critical themes of cybersecurity, characteristics, and recommendations. The aim was to reach three key audiences at the local level: city leaders, municipal managers and employees, and IT staff.

Cybersecurity has many angles: there are case studies, models, and areas of action. However, in this first edition, the guide summarizes the critical themes of cybersecurity on which the three aforementioned urban audiences should focus their attention.

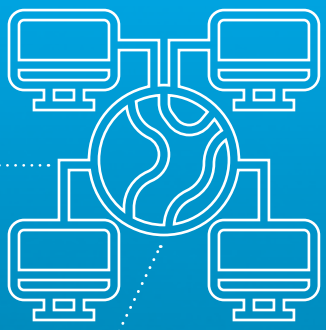


A Cybersecurity Guide for Smart Cities was financed with funds from the Cutting Edge program of the KIC Department (VPS/KIC). We are grateful for the help of Pablo Alzuri, Allen Blackman, Andrés Blanco, Janaina Borges, Hallel Elnir, Luis Manuel Espinoza, Andrea Florimon, Kenneth Foley, Jessica Guzmán Osorio, Cristina Hinojosa Lecaros, Philip Keefer, Kidae Kim, Pablo Libedinsky, Nora Libertun, Ángel Macuare Herrera, Marcelo Madeira da Silva, Fernando Melean, Santiago Paz, Daniel Peciña López, Lorena Rodríguez Bu, and Sarah Schineller for their advice and support throughout the development of the proposal, the financing, the internal processes, and the strategic communication related to the publication.

The team would also like to thank the managers and technical teams of the cities in the LAC region who, over the years, through dialogue, project implementation, and participation in studies, have shared with us their concerns for improving services in their cities and helped us create the content of the region's urban policy agenda.

Ma Zhang

Introduction



Maick Maciel

"Cities are increasingly using cyberspace, a complex infrastructure of networks of connectivity and communication interfaces, connected sensors and devices, and operational and control centers."

Introduction

The IDB presents this guide with the aim of raising awareness and understanding of cybersecurity, as well as the potential risks and results of cyberattacks on city operations. It lays out the risks, the potential impacts, and the urgent need to manage the region's cities in such a way that they can protect themselves from such attacks.

Cybersecurity must become a top priority on the agenda of city leaders and national, regional, and local governments.

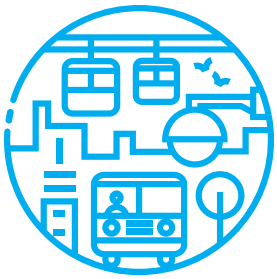

Martin Adams

What is *A Cybersecurity Guide for Smart Cities*?

This cybersecurity guide for cities and subnational governments (hereinafter, governments) provides knowledge for the cities of LAC regarding cybersecurity, digital risks, and potential impacts, and underscores the need to be proactive.

It is part of the support that the IDB offers to LAC cities in their digital transformation efforts. It complements other publications, including the following: *The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City*; *Big Urban Data: A Strategic Guide for Cities*; *Políticas públicas orientadas por datos: los caminos posibles para gobiernos locales (Data-Driven Public Policies: Possible Pathways for Local Governments)*, and *Big Data for Sustainable Urban Development (2021)*.

The guide is also part of the body of specialized knowledge provided by the IDB in the emerging theme of cybersecurity in sectors such as energy, health, water, and law enforcement. It seeks to contribute toward closing the knowledge gaps that hamper digital development. In the publication *2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean*, the IDB and the Organization of American States (OAS) provide full details on the level of maturity of LAC countries in terms of cybersecurity, as well as opportunities for improvement.

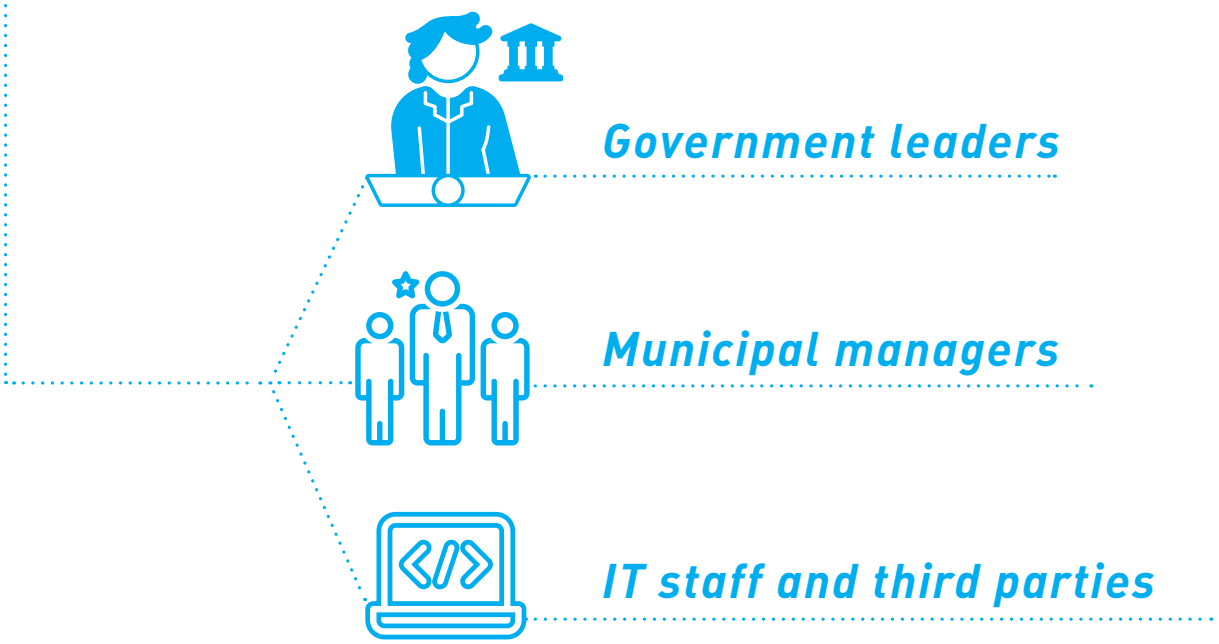


What is the guide's target audience?

A Cybersecurity Guide for Smart Cities is aimed at three types of users in cities (see Figure 1).

Figure 1.

Users of *A Cybersecurity Guide for Smart Cities*



Source: Authors' elaboration (2021).

Purpose of the Guide

The guide's objectives are as follows:

1. **Help cities** and local administrations of the LAC region to protect themselves in cyberspace.
2. **Raise awareness** and understanding of cybersecurity to safeguard information protection in every city and guarantee the continuity of services and infrastructure.
3. **Provide knowledge** about potential risks and the adoption of security measures to reduce the probability of cyberattacks and minimize negative impacts in the event of incidents.

Structure of the Guide

***A Cybersecurity Guide for Smart Cities* is organized into five chapters.** They offer a pathway to enable government leaders, municipal managers, and technical staff responsible for cybersecurity and IT, as well as third parties, to transform their cities into secure and intelligent places.

The executive summary outlines the essential structure of the elements addressed throughout the document. Chapter 1 defines cybersecurity, provides context, and describes the ecosystem, the motivations, the actors, threats, vulnerabilities, and the impact that an attack may cause at the municipal level. Chapter 2 addresses best practices, the roadmap, governance, the institutionalization of cybersecurity, the relationship with the supply chain, training, culture, and financing for cybersecurity projects. Chapter 3 offers a set of recommendations addressed to the strategic, tactical, operational, and technical staff and third-party service providers, to tackle the threats that arise from operating with the use of ICTs. Chapter 4 examines the technical capabilities needed to provide the city with cybersecurity. Chapter 5, presents the IDB's scope of action in the area of cybersecurity within the context of promoting digitalization and smart cities in the region.

Markus Spiske

Executive Summary

Fabio Hanashiro

"Optimal cybersecurity is invisible because it anticipates and eliminates problems."

Executive Summary

Mayors and city councils are leading the digital transformation of cities to provide better services and manage urban infrastructure, as well as to improve financial autonomy, sustainability, and governance.

Cities are increasingly using cyberspace, a complex infrastructure of networks of connectivity and communication interfaces, connected sensors and devices, and operational and control centers. Digitalization is accompanied by projects for smart or connected cities. Artificial intelligence and other emerging technologies are used to capture and exploit data to monitor, propose, or adopt decisions for major cities and their citizens.

With digital transformation comes targeting by hackers everywhere, including in LAC. However, most mayors, senior management, municipal staff members, and citizens are unaware of the vulnerabilities of their cities in terms of cybersecurity. Every day, there are hundreds of thousands of cyberattacks. Fortunately, most of them are repelled thanks to cybersecurity actions. Occasionally, however, the public is shocked by news that city data have been stolen or by attacks on the transportation, emergency, or law enforcement systems, or even on hospitals. Certain cities have been utterly in the grip of blackmailers and have remained inoperative for weeks (e.g., Baltimore), while in others, municipal officials have been forced to resign because they did not make the proper investments in time (Atlanta). There have even been episodes of urban violence caused by disinformation.

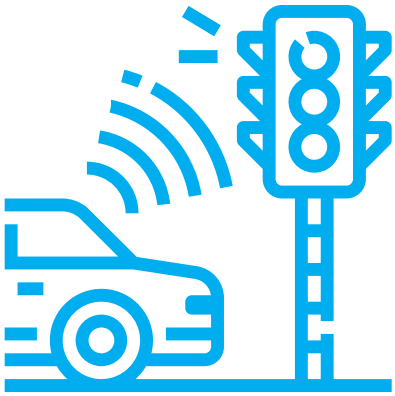
Optimal cybersecurity is invisible because it anticipates and eliminates problems. Cities must not wait for disasters to happen before protecting themselves. Attacks must be prevented and responses prepared for when they do happen. The disruption of public services and critical infrastructure carries an extremely high social, economic, political, and reputational cost for any major city.

This guide seeks to raise awareness and understanding about cyber threats to enable cities to take action. It offers what are considered to be some of the best instruments and recommendations, a roadmap to follow, and basic elements needed to be proactive in the face of cyber threats. It establishes a pathway whereby leaders, mayors and senior management, as well as employees, technicians, and third parties, can transform their cities into more cybersecure places.


Chuttersnap

The **first chapter** defines cybersecurity, cyber threats, and the impact that cyberattacks can have on cities. Cybersecurity means protecting data, information, hardware, software, services, human resources, installations, and critical infrastructure. It involves all the actors in a smart city, which means that its aim is to reduce the cyber risks or threats to which authorities, citizens, and firms are exposed when carrying out their activities or functions in cyberspace.

It is not always easy to know why cyber criminals, cyber spies, cyber terrorists, cyber activists, or anyone else launches an attack (on institutions, governments, private entities, firms, or other countries) or what their motives are (political, criminal, economic or business, or merely personal). We are vulnerable due to weaknesses in software and in often obsolete infrastructure, because we are unaware of, or fail to understand, vulnerabilities of the city's technological ecosystem. It is not a straightforward task to govern and orchestrate the numerous participating actors, or to discover and share information about security breaches or failures when they happen. Hackers take advantage of their victims' lack of strategies or their inadequate risk management and incident management plans. Human vulnerabilities, moreover, are generally even more significant than technological ones. Human resources with the new professional profiles needed are ignored or not recruited, while attacks happen especially because of a failure to raise awareness, to educate, or to offer guidance and training to managers and staff of public institutions or to the citizens themselves.



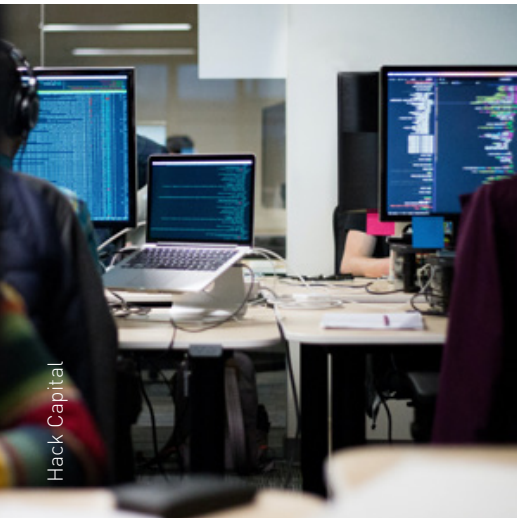
The chapter describes computer attacks that have occurred around the world and in LAC that have paralyzed cities, incurred heavy costs, and even led to the resignation of city officials. Such cases underscore the enormous importance of cybersecurity in cities and should convince those responsible for strategic, tactical, technological, or operational decisions of the need to take action. The COVID-19 pandemic has intensified the rate of cyberattacks. Vulnerabilities have increased due to people working from home with insufficient protection measures and to new forms of social engineering that have emerged from the concerns and needs caused by the pandemic. Health centers and systems have even been attacked or blackmailed, among other threats.

The **second chapter** offers some recommendations and describes best practices that compose a possible roadmap that any city can follow to achieve the highest possible level of cybersecurity. It outlines the ideal qualifications of personnel responsible for implementing these actions. Everything depends on identifying assets and actors; because of the complexity of any city that needs

protection and the many stakeholders involved, cybersecurity governance, consisting of smart city governance and the wider concept of data governance, is needed.

A city's digital security must be connected, supported, and coordinated by national cybersecurity policies and strategies, which must be institutionalized. This is often not the case. Nonetheless, any city can become a pioneer if it proactively cooperates in sharing knowledge and incorporates best practices from the international, national, regional, and local levels. By doing so, it may also be able to access better resources and sources of financing. Cybersecurity governance must be based on legislation with which it must comply. While this guide mentions some specific laws, authorities must also research benchmark standards of cybersecurity and choose those that are most suitable and achievable for the city. Starting from these bases, the strategic level must develop security policies and rules for all actors involved and establish clear responsibilities. Obviously, all stakeholders must become involved to adopt these policies and rules. Responsibility for cybersecurity should be centralized in a single person or office.

The roadmap also implies that data and information should be kept secure according to their level of risk, which is particularly the case with respect to confidential or personal data.


Hack Capital

One of the major barriers to effective cybersecurity is the lack of trust, and of instruments and platforms that permit the sharing of security information and incidents among different parties. To address this situation, some models and best practices that can be followed to better organize and exchange information are set forth below.

Public–private collaboration is essential for the digital transformation of cities and also for their cybersecurity. Therefore, this guide contains recommendations for integrating cybersecurity into the process of hiring service providers and procuring technology products and services for the city. It gives detailed descriptions of services that must be included, such as customer service, information to be shared, secure design requirements for products and services, and compliance with regulations and standards. Likewise, it presents a series of useful recommendations for choosing firms or service providers for smart cities.

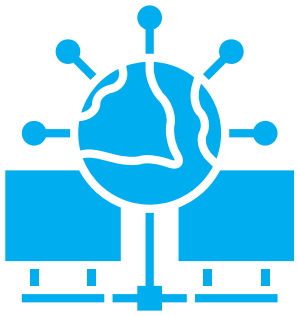
The human factor is even more important than technical cybersecurity measures. It is therefore essential to establish a culture of security, awareness raising, and training. This begins with the mayor and the city council and extends to senior management and those responsible for the smart city, plus all the employees and IT staff, and ends with the citizens. Special emphasis should be placed on communicating effectively all of the actions taken to all of the actors involved. Finally, cybersecurity undoubtedly needs financial planning. Costs will inevitably increase unless resources are allocated in a timely fashion. The possibility of taking out insurance for urban cybersecurity is also discussed.

The **third chapter** proposes three sets of rules for achieving cybersecurity for the three profiles mentioned above.


Josh Hild

First, recommendations are put forward at the **strategic level** (mayors and senior management) from an urban and a medium and long-term perspective. It underscores the need to get this issue onto the policy agenda, to enable resources to be allocated without waiting for an attack to happen, and to strengthen these actions with rules, clear authority, and the institutionalization of adequately funded leadership and agencies. Efforts should be made to put preventive measures into practice. The leadership should also have control over the private sector that provides the city with services and supplies. It is important to replace obsolete equipment with new, cyber-secure equipment. Privacy and cybersecurity must be integrated into evaluations of the smart city, and strategies must be adopted and associated with national and even international cybersecurity networks.

Second, the chapter also sets forth rules for the **tactical level** (municipal officials and employees). In this case, sound knowledge of the systems and infrastructures to be protected, and of the major threats they may suffer, is required. It therefore is useful to conduct a self-evaluation to identify any missing capabilities. Likewise, municipal officials should be familiar with the city's specific cybersecurity actions, strategies, rules, policies, and procedures. They should also be aware of their own responsibilities in this respect and should communicate with city departments and staff to make them aware of theirs. They must also ensure that the proposed measures are thoroughly tested. Officials must receive adequate training and be able to count on structured, predictable financial resources and adequately trained human resources. With regard to private service providers, obligations must be specified and, at the same time, a climate of trust created that enables critical cybersecurity information to be shared.



Finally, for the **operational level** (staff with IT-related responsibilities or jobs, staff with technological capabilities, and third-party support providers) there is also a set of rules. They include identifying the information and assets that need protecting and participating actively in an ongoing process of cybersecurity evaluation, management, and planning. The technical side is particularly important for ensuring that there are systems of identification, two-factor authentication (2FA), access control, anomaly detection mechanisms, and surveillance to ensure speedy response to incidents. All goods and services must include the corresponding security and privacy features by design and by default. It is also important to keep up to date with the methods and tools used by hackers and to have automated systems for detecting and countering threats. Likewise, hardware and software must be updated and privacy and data protection actions integrated with those of cybersecurity.

The **fourth chapter** contains a section addressed to decision-makers and technology experts. The technical aspects of cybersecurity are grouped together with a description of the cycle and steps to follow (management, identification, protection, detection, response, recovery, and self-evaluation). For readers with a technology background, the technical elements of capability-based planning are presented, as well as the roadmap and the main capability maturity models, cybersecurity functions, equipment, and technology for the day-to-day management of cybersecurity in a city. Finally, the chapter describes the responsibilities belonging to the senior level cybersecurity group.

Finally, the **fifth chapter** illustrates how the IDB coordinates cybersecurity with its vision and its activities, based on promoting smart cities at the service of their citizens. This is followed by the summary of general conclusions. The essence of cybersecurity is thus laid out: knowledge and understanding of the environment, planning, prevention and surveillance, collaboration and cooperation, and ongoing education and training. Only by adhering to these principles will it be possible to exploit the advantages of disruptive technologies to achieve more sustainable, inclusive, and productive cities and thereby improve the lives of citizens.

1 Cybersecurity, Cyber Threats, and Their Impact on Cities

NASA

"Cybersecurity means protecting data, information, hardware, software, services, human resources, installations, and critical infrastructure."

1 Cybersecurity, Cyber Threats, and Their Impact on Cities

Since the dawn of the 21st century, the use of information and communication technologies (ICTs) has become a central element for cities, for states, and for the exercise of citizens' rights. Every city has followed its own path of digital transformation toward what has come to be known as the "smart city." According to Bouskela et al. (2016), a smart city is one that places people at the center of development, incorporates ICTs into urban management, and uses these elements as tools to stimulate the design of an effective government that includes collaborative planning and citizen participation processes. By promoting integrated and sustainable development, smart cities become more innovative, competitive, attractive, and resilient, thus improving lives.

The city that needs protecting has certain fundamental elements: an urban ecosystem set in a particular region; a combination of ICT that includes infrastructure, systems, platforms, and networks; and a citizenry that interacts, exercises its rights, and seeks to meet its needs (Enerlis et al., 2012).

Such cities inhabit a new environment—cyberspace—which is "a complex environment made up of interactions between people, software, and internet services through the technological devices and networks connected to it, and that does not exist in physical form" (ISO, 2012).

Figure 1.1.

Cyberspace as a Complex Environment

Source: Authors' elaboration (2021).

1.1
What Is Cybersecurity?

Cybersecurity addresses the risks associated with providing services in cyberspace. The International Telecommunication Union (ITU, 2008) proposes the following definition of cybersecurity:

"The set of tools, policies, security concepts, security safeguards, directives, risk management methods, actions, training, best practices, insurance and technologies that can be utilized to protect the assets of organizations and users in the cyber environment."

"The assets of organizations and users are connected computer devices, staff, services/applications, communication systems, communications multimedia, and the totality of information transmitted and/or stored in the cyber environment."

"Cybersecurity ensures that the security of the assets of organizations and users is achieved and maintained against the corresponding security risks in the cyber environment."


Arlington Research

The term "cybersecurity" covers all the dimensions of digital security (OECD, 2015): (i) **technology**, when it centers on the operation of the digital environment (often called "information security," "computer security," or "network security" by experts); (ii) **application of the law** or legal aspects (for example, cyber crime); (iii) **national security**, international stability, including aspects such as the role of ICTs with respect to intelligence, conflict prevention, war, cyber defense, and so on, and (iv) **the economic and social dimension**, which includes wealth creation, innovation, growth, competitiveness and employment in all economic sectors, individual freedoms, health, education, culture, democratic participation, science, leisure and other dimensions of well-being in which the digital environment drives progress.

Cybersecurity in a smart city is the capacity of the authorities, citizens, and firms to reduce the cyber risks or threats to which they are exposed when carrying out their activities or functions in cyberspace.

Cybersecurity seeks to protect digital assets in the urban ecosystem. To achieve this aim, the following elements must be identified:

1. **Governance**, policies, and guidelines.
2. **Actors** and users.
3. **The environment**.
4. **Collaboration** and coordination with the environment.
5. **The technological tools** and instruments used to provide support for service provision.
6. **The methodologies** applied and best risk management and incident management practices.
7. **Ongoing formation** and trainings.

Two types of assets related with information security can be distinguished (ISO, 2018): main assets (business and information processes and activities) and support assets (on which the primary assets depend) of every type: hardware, software, network, staff, websites (web portals or physical infrastructure), and the structure of the organization.

1.2
Ecosystem of a Cybersecure City

The ecosystem of the cybersecure city is composed of:

i) citizens as recipients of the services;

ii) the communications platforms and networks that enable the delivery of information;

iii) the technological infrastructure and the systems that support digital service provision and the activities of cities and municipalities;

iv) connected devices, applications, data, and the information they transmit;

v) an urban ecosystem through which public services are provided; and

vi) cybersecurity capability for protecting the city's assets, that is, an authority that includes all of the above elements.

Technological infrastructure, energy supply, protection of resources, service provision, and access to good government are some of the principles that cities and municipalities seek to follow efficiently through the use of ICTs. Their use by the city must be understood in a holistic sense, so that the guarantees of cybersecurity cover each front through which cyber criminals seek to exploit vulnerabilities to achieve their objectives.

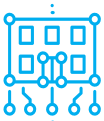
Figure 1.2.

Examples of Elements That Need Protection

Technology infrastructures
Wi-Fi networks, routers, network connecting devices, IT infrastructure.

Sensors and devices
Security cameras, mobile phones, street lighting, environmental and mobility sensors.

Data and information
Security, taxation, mobility, environmental and citizen data.



Systems and apps
Financial management and control systems, mobility and health service apps (etc.).

Source: Authors' elaboration (2021).

Martin Adams

Figure 1.3.

The Ecosystem of a Cybersecure City

Source: Authors' elaboration (2021).


Citizens
1
Cybersecurity capability
6
Urban ecosystem
5

1.3
Strategic, Tactical, and Operational Levels of Cybersecurity Management

Cybersecurity must be managed from the strategic level of city leadership, via the tactical management level of municipal officials, and reaching the operational level of cybersecurity and IT staff.

Figure 1.4.

Levels of Cybersecurity Management

Strategic

Responsible for managing, allocating resources, defining the vision, taking responsibility, prioritizing cybersecurity objectives for the city, and empowering the technical teams to lead and guide the strategies for achieving the goals. Approves the governance, regulations, guidelines and policies and the resource management that these demand. Demands compliance from all roles.

Tactical

Responsible for executing the rules. Guarantees that the teams comply with the rules, guidelines and policies, generally by defining the plans, programs and projects aligned with the priority policies. This is a specific level of management that provides detailed planning for each sector (government, mobility, health, network, etc.).

Operational

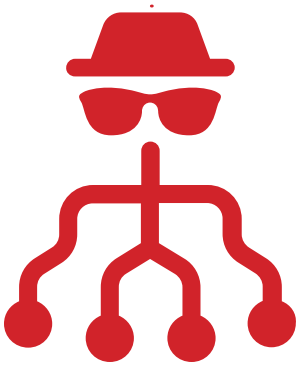
Proposes the rules, guidelines, policies, standards, and resources necessary to achieve the objectives. Proposes and executes the strategies and monitors and supervises their execution. Among other functions, proposes technical training directives and procedures for management, identification, protection, detection, response, and recovery in the event of incidents (this activity can be carried out by staff employed directly by the city or municipality, or by third parties hired by them).

Source: Authors' elaboration (2021).

1.4
Cyberattacks on Cities

When a risk materializes, a cyberattack is underway, which harms or jeopardizes, among other elements, data, information, infrastructure, and generally any of the assets described in Section 1.1 of this guide.

The following section examines the main actors and motives behind the launch of a cyberattack. It also explains the main types of attacks and vulnerabilities and the effects observed when a cyberattack targets a city or municipality.



1.4.1
Main Actors and Motives for Launching a Cyberattack

There are various motives for launching an attack: to satisfy a personal challenge, obtain privileged business or government information, pursue a political objective, or obtain an economic reward. These motives are not mutually exclusive. For example, a cyberattack may conduct criminal spying activity for both business and political ends.

Any of these motives may be an excuse to put municipalities at risk. These motives might be shared by one or more actors, as will be seen below.

Figure 1.5.

Motives for Launching a Cyberattack on a City

Personal

The attacker wishes to satisfy a wish, need, or any other similar desire. Personal growth, accepting a challenge, curiosity, revenge, personal satisfaction, among others, may all constitute a motive for launching a cyberattack.

Criminal

Criminal motivation may be linked to two objectives: causing harm or damage or jeopardizing the victim's legal assets; or obtaining a profit from such conduct for the criminal or third parties.

Business

Gaining inside information, business secrets, or knowledge of other business activity or of the infrastructure that supports services and, in general, the supply of goods and services, can all be motives for carrying out a cyberattack.

Politic

Criminal motivation may also be linked to changing the political regime, bringing down a democratic sector, influencing citizen decision-making, or jeopardizing or destabilizing a nation's sovereignty, government, territory, or population.

Economic

Carrying out a cyberattack may provide returns, compensation, profits, or earnings for the attacker or a third party.

Other

There are other possible motives. There may also be motives that intersect. An example might be carrying out criminal activity to gain revenge, but, at the same time, having a business or economic motive.

Source: Authors' elaboration (2021).

Every cyberattack involves a series of actors, victims, and victimizers. The role of each actor is detailed in Figure 1.6.

Figure 1.6.

The Main Actors in Cyberattacks

Active

Those who, for different reasons, carry out cyberattacks, either directly or indirectly:

- Cyber **criminals**
- Cyber **spies**
- Cyber **terrorists**
- Cyber **activists**

Passive

The victims of the cyberattack:

- **Citizens**
- **Firms** and private organizations
- **The state** or any public authority, such as municipalities

Whatever the type of actor (active or passive), these may be:

Public	**Private**	**Nationals**
Foreigners	**Individuals**	**Collectives**

Source: Authors' elaboration (2021).

The types of threats to which a major urban ecosystem may be subjected can be understood depending on the roles played by each of these actors.

1.4.2
Main Types of Attacks and Vulnerabilities

The objects of a cyberattack may be information, hardware, software, service provision, networks and connections, human resources, critical cyber infrastructure and, in general, any city asset or service that uses ICTs. The most frequent attacks involve the use of social engineering, malware programs, brute force to obtain access, and attacks on connections and infrastructure. Such actions seek, among other goals, to threaten the privacy, integrity, or availability of information systems and circumvent security measures.

Urban and municipal authorities must be aware of the most frequent techniques (also known as hacking techniques) used and the main types of threats. Figure 1.7 summarizes some of them.

Figure 1.7.

Most Common Types of Threats and Cyberattacks

Ransomware
Activity by which hackers take control of a device and encrypt the information. In some cases, the information is leaked under threat of publication. In exchange for recovery of control and information, a ransom payment is demanded.

Distributed denial of service (DDoS) attack
Attack on a server or network simultaneously from many different devices with zombie networks so that the server crashes as it cannot deal with so many requests.

Wi-Fi honey pots
Creation of a parallel Wi-Fi network to a legitimate and secure one, with the same or a very similar name to the original, to steal data from anyone connecting to it.

Phishing
Sending messages masquerading as an identity that seems to legitimate, in order to gain access and attack.

Mail spoofing
Using the forged email address of a trusted person or entity in order to steal personal information transmitted under false pretences.

Zombie / botnets
A number of different zombie devices infected and controlled together by cyber criminals.

Social engineering
Set of techniques aimed at psychologically manipulating users to take compromising actions such as, for example, revealing personal information or by surfing malicious websites, which enable the hacker to take control of devices.

SQL injection
Attack on a web service based on SQL language, compromising the database through malicious source code and exploiting vulnerabilities in its programming.

Spam or junk mail
Sending huge quantities of unsolicited messages or publicity over the internet.

Trojans
Virus used to control a computer, steal the data, introduce more malicious software into the device, and spread to other devices.

Malicious advertising
Seeks to gather information about the user's activity and, in this way, show directed advertisements. Its installation can lead to poor computer performance and malfunction.

Man in the middle
Also known as an intermediary attack. Here, the malicious intermediary interrupts a conversation between two assets and intercepts the communication, thereby gaining access to read or manipulate any data, messages, credentials, or transfers that are exchanged.

Source: Authors' elaboration (2021).

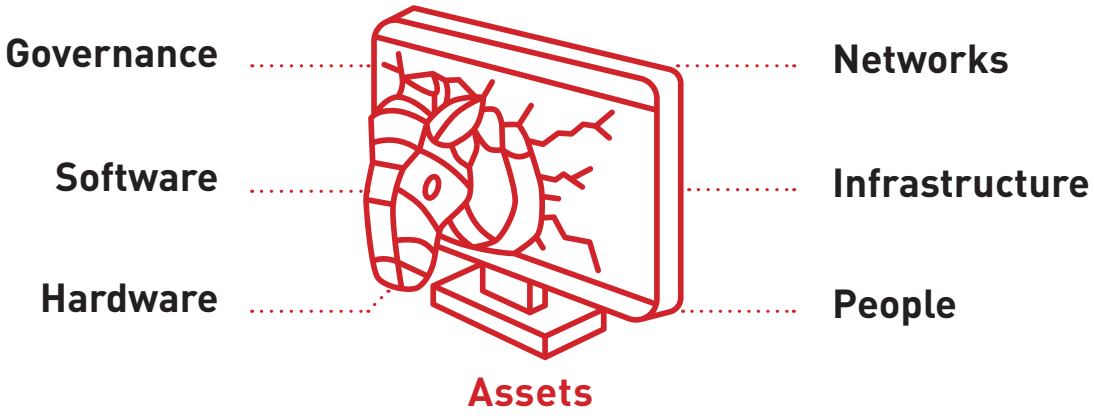
Other techniques or methods of attack include a data analysis attack, malicious applications, cookie poisoning, DNS cache poisoning, IP address spoofing, port scanning, false antivirus programs, worms, backdoors, keylogging, spy software, website spoofing, ransomware, stealing confidential information, cyber-physical attacks, and crypto mining, among others. All of these actions may be combined with others, and their results can be devastating.

Cyberattacks can take place because there are vulnerabilities, that is, faults in the assets (software, hardware, networks, and infrastructure), in the interaction between the assets, or in governance. Furthermore, the **human factor** is one of the main weaknesses that cyber criminals exploit to achieve their objectives. These may have their origin within organizations or outside of them through supply chains and other third parties (customers, monitoring authorities, etc.).

The implementation of permanent controls is therefore essential, alongside the identifying vulnerabilities, ongoing training, collaboration between actors and appropriate risk and incident management, each one of which are major activities involved in protecting an organization's assets.

Figure 1.8.

Origin of the Main Faults and Vulnerabilities



Source: Authors' elaboration (2021).

Cyber criminals exploit faults and vulnerabilities in cities, which are linked to the following defects:

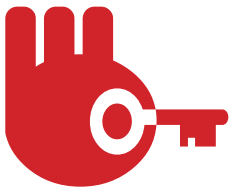
1. **Absence of an integrated cybersecurity strategy.**
2. **Lack of cybersecurity governance, rules, guidelines, and policies.**
3. **Lack of full integration of the supply chain and the third parties that relate to the city throughout the cybersecurity process.**
4. **Lack of a data protection policy.**
5. **Lack of adequate vulnerability, risk, and incident management.**
6. **Failure to update the software and hardware deployed for the city's service provision.**
7. **Faults in the software and hardware deployed.**
8. **Lack of training and formation of staff and other stakeholders (third parties, users).**
9. **Lack of economic resources to develop the city's cybersecurity strategy.**
10. **Lack of cooperation and collaboration between the different authorities and the private sector.**
11. **Lack of capabilities (human resources, tools, and technologies).**
12. **Failure to understand the digital environment.**
13. **Nonexistent or erroneous application of technical controls.**

Los riesgos materializados a través de los ataques generan consecuencias como las siguientes:

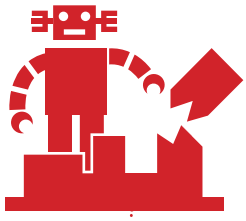
1.4.3

Possible Consequences of a Cyberattack on a City

When risks become reality through an attack, there may be a variety of consequences:



- **Interruption of critical city services** such as energy, water supply and treatment, transportation, health, traffic control, and so on.
- **Decline in worker productivity.**
- **Suspension of municipal revenue collection.**
- **Interruption of service** provided to citizens, such as completing procedures or granting licenses, among others.
- **Reputational damage** to the municipal administration and subsequent mistrust.
- **Violation of data privacy and confidentiality laws**, which can lead to investigations and sanctions.
- **Loss of investments** already made for service provision.
- **Political, economic, or social destabilization.**
- **Undermining of data integrity, availability, confidentiality, and authenticity.**



1.5

Computer Attacks That Have Paralyzed Cities

Giacomo Carra

Christian Wediger

According to the taxonomy of cyber harms proposed by Agrafiotis (2018), these comprise five general classes: (i) physical or digital harm, (ii) economic harm, (iii) psychological harm, (iv) reputational harm, and (v) social harm. These harms may be connected and, according to the attack, there may be high or low propagation. Hundreds of thousands of cyberattacks happen every day, many of them on cities and other types of critical infrastructure.[2] Fortunately, the vast majority are unimportant, thanks to cybersecurity. Since 2003, there have been around 1,000 cyberattacks, each of which has generated costs of more than US$1 million (CSIS, 2021), and there were more than 500 significant ransomware attacks in 2020 and 2021.[3]

Some years ago, the **April 2007 cyberattack on Estonia was the turning point that caused governments and cities to begin to take cybersecurity seriously**. Following the controversial removal of a statue, there was an avalanche of access requests (a DDoS attack) that crashed the country's internet network and blocked access to servers, banks, newspapers, and numerous government electronic services. More than a million computers were used to launch this attack, which downloaded malicious software after their users visited a certain webpage or opened an email that converted them into remote-controlled zombies used to connect to the same point and bring about its collapse. On the positive side, the **situation also affected the North Atlantic Treaty Organization (NATO) and was a catalyst for the European Union and international institutions to implement cybersecurity measures**. Likewise, since that time, the government of Estonia has fully understood the importance of a cybersecurity strategy and the need for government leadership and collaboration between the State, industry, and academia. Primarily in response to this attack, **Estonia became one of the world's most advanced countries at the digital level.** In this case, the harms were social, digital, and economic.

2. See https://www.sicherheitstacho.eu/start/main, https://cybermap.kaspersky.com/es, https://www.fireeye.com/cyber-map/threat-map.html, https://horizon.netscout.com.

3. See https://cloudian.com/ransomware-attack-list-and-alerts.


Bermix

The goal of the most notorious cyberattacks of recent years has been to attack the political, emergency, transportation, or policing systems of major cities. In April 2021, hackers stole more than 250 GB of extremely sensitive information from the Metropolitan Police Department in **Washington, D.C.** (MPDC). As proof of their success, they disclosed some of the information, demanding money and threatening to "make contacts with gangs to expose police informants." The protagonist on this occasion was ransomware. This attack followed the pattern already initiated in June 2017, when the hackers managed to set off storm and disaster warning sirens in **Dallas**, Texas, leading to the collapse of emergency telephone lines. In January 2017, criminals managed to take control of the security cameras of the MPDC for four days. In November 2017, the Regional Transit System of Sacramento, California, suffered a cyberattack that resulted in the loss of program information and data needed for bus operation and route planning.


Nataniael Melchor

Health systems have also been an important objective, which has been very costly. In January 2020, a cyberattack on the University Hospital of Torrejón, in **Madrid**, Spain, damaged many of its computer systems (digital harms). This line of attack had already been tried some years previously, with one noteworthy incident occurring in May 2017, when London's hospital network suffered a ransomware attack on its computers that affected hospitals, health centers, and patients. It also affected the ambulance network. Medical staff were unable to access the clinical histories of their patients, and citizens' lives were put at risk. Thousands of appointments were cancelled, and emergency patients had to be relocated. It is estimated that this attack cost GBP 92 million (US$130 million).[4]


Brad Huchteman

Atlanta, Georgia (United States): a city collapsed and a government forced to resign for failing to invest in cybersecurity in time. In March 2018, hackers managed to crack passwords in **Atlanta**. This affected many of the city's services and programs for several weeks, including car parks and legal services. The city's civil servants had to revert to filling out forms by hand. Before the attack, the government of Atlanta had already come in for criticism for its scant spending and shortcomings in cybersecurity. Failure to invest in time had a subsequent enormous political and economic cost. The situation therefore led to the resignation of dozens of civil servants and the entire cabinet. To recover, Atlanta was forced to invest US$2.7 million.

4. See https://www.acronis.com/en-us/articles/nhs-cyber-attack.


Colin Lloyd

Colonial Pipeline

The ransomware attack on **Baltimore, Maryland (United States)** was catastrophic. In May 2019, a ransomware attack blocked computers, systems, and emails, among other assets of the Mayor's Office. The hackers demanded a payment of 13 bitcoin (approximately US$76,280) from the city government, but the Mayor refused to pay it.[5] This decision cost the city an estimated US$18.2 million. Baltimore could not function normally for three weeks, and it did not fully recover for several months.

In August 2021, hackers stole data from the **Mayor's Office in Santa Fe de Antioquia, Colombia** and used it for the purpose of extortion. Consequently, citizens were unable to complete procedures online, and municipal accounts were frozen. Likewise, in March 2021, the **State Public Employment Service (Servicio Público de Empleo Estatal, or SEPE) in Spain** was attacked by the Ryuk ransomware, which complicated management and delayed payment of unemployment subsidies for three weeks. The salient fact in this case was that failure to update the computer systems had made the attack possible. In May 2021, the **United States government** declared a state of regional emergency due to the ransomware cyberattack on the **Colonial Pipeline** system, one of the country's main oil pipeline networks. The attack managed to disconnect the technological infrastructure of the pipeline, which extends for more than 5,500 miles between Texas and New Jersey and transports 45 percent of the diesel, gasoline, and airplane fuel on the east coast of the country. This was a ransomware attack that demanded money in return.

In December 2019, the government of the province of **San Luis, Argentina**, was forced to declare an emergency for 90 days after its filing system was blocked and a ransom demanded. The city refused to pay and did manage to recover information until December 2018, but encountered significant problems when it came to decrypting the 350 GB corresponding to 2019. For its part, in February 2020, **Mexico's Economic Secretariat** was forced to suspend administrative terms and deadlines after a cyberattack infected files and emails.

5. Available at https://twitter.com/mayorbcyoung/status/1136377418325864448.

In June 2021, the **El Bosque University in Bogotá** announced to the entire academic community that it had been prey to a cyberattack, which meant that some of its internal systems had been compromised. Presumably, this attack was carried out using a distributed denial of service and, as a result, administrative and academic activities were blocked for several days.

A story with a happy ending—thanks to foresight. In June 2021, the New York City subway system suffered a computer attack. The Metropolitan Transit Authority (MTA) had already established a robust cybersecurity strategy, which enabled it to contain the attack and maintain services. It appears that the planning and the multiples layers of the MTA were able to function according to the design. Furthermore, in the months prior to the attack, following several attacks against critical U.S. infrastructure, extra sensitivity to threats had been developed, alongside elements of foresight.

Following COVID-19, new forms of cyberattacks have emerged. Social engineering, the extreme need for essential supplies and information related to COVID-19, began to be used as a signal for obtaining data and conducting fraudulent activities and phishing. Computers were hacked through malware, malign attachments, and identity spoofing. There were also ransomware and DDoS attacks against hospitals and medical centers, which became overloaded. Similarly, vulnerabilities related to telework were exploited to steal data, make money, or cause malfunctions (Interpol, 2020). Thus, for example, in March 2020, in **Costa Rica**, a ransomware application known as COVIDLock spread throughout the country and also affected the public sector. The application theoretically provided interactive maps showing the extent of virus propagation, but thereafter exploited the users' interests to hack their computers and demand bitcoins (economic and social harms).

1.6

Cybersecurity Maturity in Smart Cities

As the National Institute of Standards and Technology (NIST)[6] (NIST, 2019) concluded, smart cities and communities are neither sustainable nor truly intelligent if they fail to proactively identify, deploy, maintain, and adapt the processes and measures of cybersecurity and privacy risk management. Doing so creates trust and facilitates participation in the smart city.

In its Measure 7, the European Union Agency for Cybersecurity (ENISA, 2015) points out that smart cities and standards agencies must adapt cybersecurity to the level of urban maturity. The most mature cities would therefore demonstrate their security measures, while less mature cities would be encouraged to improve.

However, there is insufficient awareness-raising. The most respected international digital maturity rankings for cities fail to include cybersecurity. These include: IMD-SUTD Smart City Index (SCI),[7] Top 50 Smart City Government Rankings (smartcitygovt),[8] Smart City Winners, IESE's Top 10 By Dimension,[9] JUNIPER Research 2019–2023,[10] among other.

A possible way to improve this situation. The IDB has begun to integrate security and privacy, on the one hand, into the five levels that measure the degree of maturity of smart cities (Townsend and Zambrano-Barragán, 2019: 19 and following). Furthermore, security and privacy are one of the four dimensions of the assessment of big data maturity for urban development (Biderman et al., 2021). Recently, the G-20 roadmap for "pioneer cities" added security and privacy as essential elements (G-20 Global Smart Cities Alliance, 2021), while in Japan (MIAC, 2020) privacy and security are also basic elements.

6. The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand their cybersecurity risks, manage and reduce such risks, and protect their networks and data.

7. See https://www.imd.org/smart-city-observatory/smart-city-index.

8. See https://www.smartcitygovt.com.

9. See https://smartcity.press/top-10-smart-cities-of-2020.

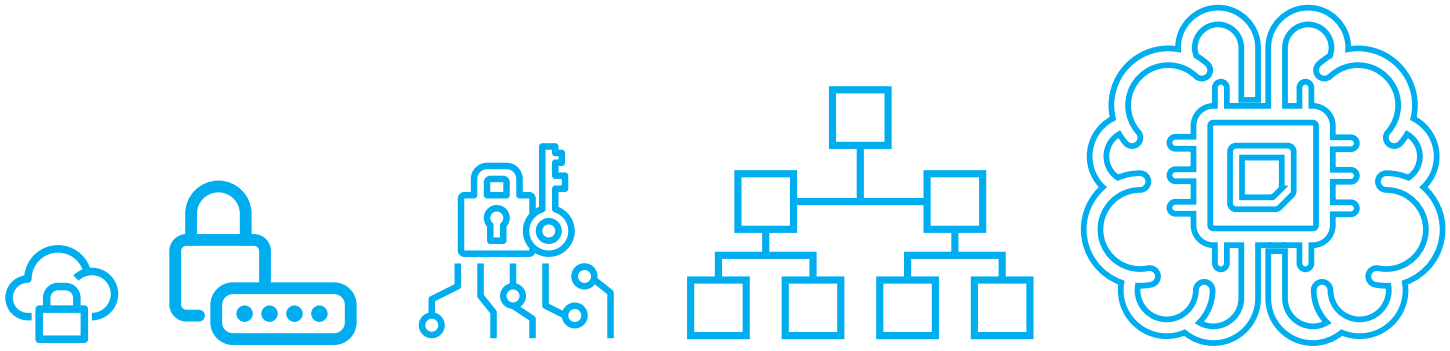
10. See https://www.juniperresearch.com/researchstore/key-vertical-markets/smart-cities-research-report/subscription/leading-platforms-segment-analysis-forecasts.

The G-20 Global Smart Cities Alliance for Technology Governance, which links municipal, regional, and national governments to private sector partners and civil society, was created in 2019 to gather and analyze successful and ethical policies for smart cities. It already has a political governance model (G-20 Global Smart Cities Alliance, 2020) and a roadmap (FEM, 2021), within which cybersecurity has been incorporated as a cross-cutting element.

Through joint work by the IDB and the OAS (IDB and OAS, 2020), a Cybersecurity Capacity Maturity Model for Nations (CMM) was applied in Latin America and the Caribbean. This model, elaborated by the Global Cyber Security Capacity Centre of the University of Oxford, evaluates the level of maturity of a country's cybersecurity capabilities in five stages: (i) initial, (ii) formative, (iii) consolidated, (iv) strategic, and (v) dynamic.

Figure 1.9.

The Five Stages of Cybersecurity Maturity

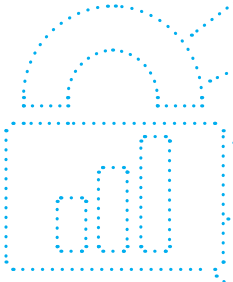


Source: Authors' elaboration (2021).

In turn, evaluation of the levels of maturity is divided into five dimensions: (i) cybersecurity policy and strategy; (ii) cyber culture and society; (iii) cybersecurity education, training, and capabilities; (iv) legal and regulatory frameworks; and (v) standards, organizations, and technologies. These are divided into a set of factors that describe and define what it means to possess cybersecurity capability in each factor and indicate how maturity might be increased. The indicators and the model are also useful and serve as references for cities.

Figure 1.10.

The Five Dimensions of the Cybersecurity Maturity Model (CMM)



1. Cybersecurity **policy and strategy**
2. Cyber **culture and society**
3. Cybersecurity **formation**, training, and skills
4. Legal and regulatory **frameworks**
5. **Standards**, organizations, and technologies

Source: IDB and OAS (2020: 42).

The reports (IDB and OAS, 2016, 2020) detected a significant increase in interest in and awareness of cybersecurity, as well as a substantial increase in maturity in this field, as measured by greater capacity on the part of the authorities and the elaboration of national strategies and legislation. The region's countries are on the way toward digital transformation with cybersecurity, and their challenge is to ensure that cities can implement many of the elements presented in these reports.

In the process of migrating to smart cities and the use of urban big data, it is essential to incorporate capabilities that can help create an adequate level of cybersecurity. Likewise, implementing cybersecurity must be prioritized so that the services offered in the city are cybersecure.

Markus Spiske Iar

2 Recommendations and Resources to Protect Cities from Cyberattacks

Daniel Lloyd Blunk Fernández

"A city's technological architecture and infrastructure are complex; the actors that intervene are heterogeneous, as are the information and the data to be protected."

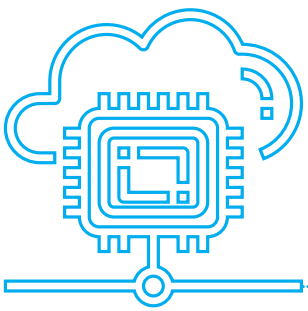
2 Recommendations and Resources to Protect Cities from Cyberattacks

Readers of this guide are already aware of the concept of cybersecurity and of the threats that can seriously harm cities in cyberspace. The way to protect cities from cyberattacks is to take proactive measures to strengthen cybersecurity. Some years ago, the IDB (Bouskela et al., 2016: 115) published *The Road Toward Smart Cities*, which proposes a cybersecurity roadmap for cities. Figure 2.1 contains this roadmap with the recommendations, practices, and resources needed for a risk management-based approach to protect any type of city.

Figure 2.1.

Roadmap to Urban Cybersecurity

1. **Identify** assets and actors that require protection.
2. **Establish** cybersecurity governance.
3. **Institutionalize** cybersecurity.
4. **Integrate** city confidential data and personal data security.
5. **Integrate** service providers and cybersecurity.
6. **Train**, communicate, and raise awareness of cybersecurity.
7. **Provide** resources for cybersecurity finance and insurance.



Source: Authors' elaboration (2021).

A city's technological **architecture and infrastructure** are complex; the actors that intervene are heterogeneous, as are **the information and the data** to be protected. The first step, therefore, is to identify all these elements (NIST, 2019). The city's tactical and technological staff is responsible for this task. Based on the knowledge of the complexity of cities and their citizens, the strategic level must establish **governance** that fully integrates cybersecurity management, the smart city, and data. As a premise, the mandatory laws and rules regarding monitoring must be observed, for which the tactical level provides fundamental support. Likewise, the technological staff must choose among the cybersecurity standardization and certification schemes on offer. On this basis, the strategic level should establish common security policies and rules for the city, with clear responsibilities and stakeholder participation. Likewise, urban cybersecurity must be connected with national policies. Establishing governance means **institutionalization** by the strategic level. It must appoint a person responsible for cybersecurity, with the specific functions that are described herein. The best practices for ensuring that the tactical and technological levels share security information will also be found in these pages.

Information and data must be protected. In general, within legal parameters, the tactical level identifies whether there is confidential and personal data that requires special protection, while the technological level provides the corresponding protection. Among the most important best practices in this respect are to anonymize (and pseudonymize) and encrypt the data managed by the city.

Likewise, the **choice, management, and procurement of suppliers and service providers should be integrated into cybersecurity**, an essential task of the staff at the tactical level. Among the most significant recommendations and best practices are **the culture of cybersecurity, awareness-raising, and training** for managers and city employees. Finally, it is essential to provide a cybersecurity budget and to examine whether insurance should be purchased. This requires leadership from the strategic level, alongside tactical support.

Zhang Kaiyv

2.1
Identify the Assets and Actors to Be Protected

As things stand today, the use of ICTs for providing services and managing urban infrastructure is essential in any major city. However, ICT deployment implies managing the risks that this entails. As mentioned in the previous section, many cities have seen their service provision capacity paralyzed due to multiple cyberattacks.

To begin with, it is vital to **identify what needs to be protected, that is, the main assets (business processes and activities and critical data) and the support assets** for that information (**hardware, software, network, staff, structure of the organization**, etc.), for which security must be provided, and to measure the level of possible impact from a cyberattack.

All of the intelligent elements supported in cyberspace and unprotected should be taken into consideration: intelligent industrial systems (SCADA networks), for example, electrical distribution systems; city surveillance systems and environmental variable sensor systems that sustain the internet of things (IoT). The presence of these devices means that the perimeter to be protected becomes practically unlimited. In the city ecosystem, in addition to the most common IoT technologies, numerous heterogeneous technologies also coincide: diverse communications protocols, cyber-physical mechanisms (controlled by algorithms and integrated with the internet), robots, drones, and autonomous vehicles. And all work in consonance with connected cloud-computing technologies, big data, and artificial intelligence (AI). Moreover, it is also essential to identify and consider the interdependencies between systems, given that a low-risk system may be linked to others or might be high risk in a different context. Likewise, according to ENISA (2015), another problem to consider is caused by the long life cycles of the equipment used or by inherited systems, whose design rarely incorporates adequate security features. This must be resolved by an investment plan (OSPI, 2017).

The broad range of interacting public and private stakeholders that require orchestration and governance should be mapped, including:

- Senior management.
- The most specialized sectors of the city in terms of technology, cybersecurity, and data protection.
- Areas with responsibility for security (police security, labor, etc.).
- Sectoral areas most implicated in digitalization (finance, transport, waste, health, supplies, etc.).
- Cooperation or coordination superstructures created at the local, regional, or national levels.
- Those responsible for the different service layers, infrastructure, communications, and so on, which are often providers of services and communications to third parties and, generally, private actors (water, electricity, mobility and transport, security, etc.).
- Public sector entities that are sometimes both service providers and service recipients.
- Tertiary sector, nongovernmental organizations (NGOs), or academia, which may be integrated into processes of analysis or participation (Muñoz et al., 2016: 26).
- Citizens, who are service users and at the same time owners of the data that feed the city, and those who suffer from attacks or service failures.

Christina Wocin

2.2
Establish Cybersecurity Governance

Following identification of the assets, data, and processes to be protected and of the actors that need to be coordinated, a clear scheme of cybersecurity governance must be established.


Mahdis Mousavi

2.2.1
Establish the Cybersecurity Governance Scheme and Integrate It with Governance of the City

Cybersecurity governance should be integrated with governance of the smart city, which implies creating rules and policies, as well as building an organizational structure (MIAC, 2020). According to the World Economic Forum (WEF) (WEF, 2021), governance of the smart city presupposes the integration of five policies:

1. **Accessibility**, inclusion and social impact
2. **Security** and resilience
3. **Privacy** and transparency
4. **Openness** and interoperability
5. **Open data policy** and so-called Dig Once policies, to guarantee that digital infrastructure is installed with operational and financial sustainability

The direction and management of the city and the smart city can be seen as the treatment and mass exploitation of enormous quantities of data. Governance of the city—and of its cybersecurity—must be integrated with the broader sense of **data governance**. This implies, among other actions, **establishing the data sources, organization and traffic, institutions and agencies, competencies and responsibilities, and management guidelines**. It is important to identify the necessary data and the sources from which they are taken and to determine where the data will be integrated, compiled, cleansed, and sorted, and subsequently analyzed and interpreted. Cybersecurity governance must include data governance. This means establishing responsibilities with regard to decision-making about updating, access, availability, ownership,

security, and privacy. Similarly, this implies setting the guidelines and rules of data management, its quality, and its uses. Governance requires managing the data architecture and infrastructure, as well as interoperability and the protocols that facilitate data exchange, both internally and externally, with other administrations or with private entities. Data governance also permits professional skills and human resource management to be redefined and helps to attract or incorporate people with the appropriate skillsets. Likewise, it permits transformation of the management model and encourages a culture change for the entire ecosystem.

With respect to innovation and the smart city, the IDB has underlined the **importance of appointing leaders**, which creates a culture of data governance, and of establishing democratic innovation authorities (Townsend and Zambrano-Barragán, 2019). **Creating institutions of governance, or their regulation, sends an explicit message about the importance of this issue.** Likewise, a trend can be created toward centralizing the criteria and methodologies of data gathering, treatment, and exploitation and establishing shared data archives. This can also help to decentralize specific actions with respect to different sectors, thereby facilitating coordination and interoperability and encouraging cross-cutting trends (Salvador, 2021).

Data Governance Examples to Follow:

- **Creation of agencies: the Mayor's Office of Data Analytics (MODA) of New York and the Citywide Analytics Team of Boston, created in 2015; the London Office of Data Analytics (LODA) of 2017. In Spain, the Municipal Data Office (OMD) (Oficina Municipal de Datos) of Barcelona City Hall, set up in 2018, and (at the national level) the Division Data Office (División Oficina del Dato), put into operation in July 2020.**

- **As a regulatory example, Decree 76/2020 of August 4, 2020, approved in Catalonia, regulates governance of digital administration (Arts. 5–9), as well as data governance (Title II, Arts. 10–26: model, protocol, exchange, interoperability and access to data, digital processes and services, data archive, and digital asset management).**

The rules and the standardization and certification schemes to be followed to achieve a secure city must be integrated, and they must also be aligned with regional and national policies. **It is important to establish whether a national cybersecurity strategy exists in the country.**

In 2004, the General Assembly of the OAS approved the Inter-American Strategy to Combat Threats to Cybersecurity (Barrero et al., 2018: 116). Many of the region's countries have adopted national cybersecurity strategies (Argentina, Brazil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, Mexico, Panama, Paraguay, the Dominican Republic and Trinidad and Tobago) (IDB and OAS, 2020: 180).


Eddie Kopp

In general, and unfortunately, these strategies do not take cities into consideration or apply directly to them. However, **urban cybersecurity also forms part of national cybersecurity**. The G-20 Global Smart Cities Alliance (2021) states its concern for the "poor connection with national policies" of local cybersecurity. Soare and Burton (2020) speak of the "missing link" between the smart city and national security. ENISA (2015) recommends that the "European Commission and the member states define the responsibilities of each agent in the event of a cyber incident," and the NIS Directive (Directive 2016/1148) of the European Union takes a similar line. The connection between preparing for subnational security and national or federal responsibility was the object of analysis in the 2017 report by the National Association of Governors in the United States (García, Forscey, and Blute, 2017). For their part, New America, Cohen, and Nussbaum (2018) recommend a federal response to financing to connect regional or local programs with national priorities and rationalize them. It is also worth remembering that relationships between regional authorities and cities can be equally or even more fractious than those with national or federal authorities.

This situation will need to be remedied from the regional and national levels. However, it may even represent an opportunity for cities. **Cities can be proactive and attempt to connect urban cybersecurity with national cybersecurity.** For this purpose, the national—or international—cybersecurity channels or networks must be identified. Readers with responsibility in this matter should consider that their city could become a pioneer in this field. It is possible to participate in or promote networks of best cybersecurity practices among cities. It may even be possible to find cybersecurity financing programs.

The city must be aware of the cybersecurity legislation it is required to follow. Each country may have different regulations on cybersecurity. If such regulations exist, cities or those who provide services and supplies (in telecommunications or technology) must comply with them. The European Union has sought to establish homogeneity and common European standards of cybersecurity. The NIS Directive requires all member states to adopt a national strategy and to impose obligations on essential service providers and critical operators or, in other words, those whose failures might lead to financial losses, undermine people's trust, or even pose a threat to national security. These service providers who must adhere to these requirements often operate and provide services to cities. They should be encouraged to adopt measures according to the levels of risk, based on a prior evaluation of the same. Thus, for example, such service providers and operators are required to notify cybersecurity incidents, even though they had no real effect, as a way of promoting the culture of risk management. There is a common reporting platform that could also be used to report breaches of personal data security. The system is confidential and protects the notifying entity and any staff who report incidents, which could also involve the city. The competent authorities will exercise monitoring functions and promote the development of these obligations.

In Spain, the public sector and cities are required to comply with the National Security Scheme (Royal Decree 3/2010, January 8, 2010) and the Security Guides. If the city lacks legislation, the scheme and these guides can provide a useful reference. Likewise, the NIS Directive has been issued mainly through Royal Decree-Law 12/2018, September 7, 2018, relating to network and information system security, while Royal Decree 43/2021, January 26, 2021, has specified obligations, security measures, and requirements.

Singapore launched its national cybersecurity master plan in 2013, followed by new draft legislation on cybersecurity in 2016, which was approved and went into effect in 2018. Both initiatives were part of Singapore's Smart Nation Strategy, one of whose pillars is cybersecurity.[11]

Beyond any mandatory legislation, the technological team must be aware of the various standards of cybersecurity, privacy, and their adaptations for the IoT, telecommunications, and smart cities and must opt to follow one of them to the extent possible. In recent years, more and more commonly accepted standards and rules, as well as best practices, have been developed. The standard framework of the sector should be followed to guide the organizations' cybersecurity and risk management policies, such as ENISA or NIST, as well as ISO 2700, AICPA, CIS, or COBIT. Likewise, the team must pay particular attention to cybersecurity standards for the IoT and telecommunications issued by these organizations, the European Union, or NATO. Specifically with respect to the smart city, the International Standards Organization (ISO) had already made ISO 37120 available, with indicators for urban services and the quality of life. In 2017, ISO 37121 was adopted for sustainable development and resilience in cities, alongside ISO 37120, as a template for the development of smart cities. In 2019, ISO 37122 was adopted, with indicators of progress in smart cities in terms of the economy, education, energy, sustainability, finances, governance, health, housing, population and social conditions, recreation, security, waste disposal, sports and culture, telecommunications, transportation, urban agriculture and food security, and spending on water provision. The specific standards of security for the public sector and the city may also be used. The technical section in Chapter 4 presents the basic guidelines that a city can follow based on these systems.

11. See https://www.smartnation.gov.sg/about-smart-nation/secure-smart-nation/cybersecurity-public-sector.

In 2000, ISKE was created. It is a security standard for the implementation of organizational and infrastructure standards and technical security measures in Estonia's national and local public sector (Information System Authority, 2021).

Since 2012, Spain's Technical Standards Committee 178, of AENOR, for smart cities and its six sub-committees (infrastructure, indicators and semantics, mobility and transportation platforms of, energy and environment, tourist destinations, government and public services 4.0) has published 31 rules for smart cities (UNE, 2021). These rules facilitate smart city management and strategies and help document the state of repair throughout the entire life cycle of the city's assets and technological infrastructure, and the risks and possible responses.

Since 2010, Stockholm, Sweden, has been implementing mandatory internal directives on information security that adhere to ISO/IEC 27002. It carries out numerous cybersecurity awareness-raising activities and implements educational programs, while offering support for research and innovation laboratories for start-ups.

In 2014, the area of Rennes St Malo, France, was certified with the French Tech seal of approval as a French Technological Capital (La French Tech, 2019), since it occupies first place in telecommunications, agro-industry and cybersecurity. It launched the international Rennes Metropole innovation program with strong business and research partnerships (Eurocities, 2016).


Dimitrina Kolarova


John Loannidis

2.2.2

Develop Common Security Policies and Rules with Clear Competencies and Stakeholder Commitment

Based on the applicable legislation and existing standards and models, a city should have governance that integrates data, the smart city, and cybersecurity.

In Measure 5, ENISA (2015) recommends that operators, cities, and anyone seeking to improve the security of their processes and services establish responsibilities for senior management in the area of cybersecurity. Defining responsibilities in this way can be an incentive for improving cybersecurity. Likewise, New America, Cohen, and Nussbaum (2018) stress the need to clearly define functions, responsibilities, and authorities. This regulation must be a clear indication of leaders' support for cybersecurity initiatives, and must reduce possible confusion and conflicts. An integrated and centralized program is required for all stakeholders, not just those in the technological area. Conflicts between different agencies when incorporating cybersecurity into processes are common. However, this problem could be solved by a cybersecurity superstructure or by a coordinator or advisor in these matters.

In this regard, Japan (MIAC, 2020) recommends the following:

I. That cities should develop rules for cybersecurity management, data treatment policies, and risk criteria that are common to all.

II. That cities should define the competencies of all stakeholders; there must be prior agreement about which organization is responsible for logging the incidents and which one must respond. Otherwise, service provision could be blocked. Both a configuration diagram and a system diagram should be made, and management white spaces should be eliminated.

III. That all stakeholders are aware of, and have deliberated, points I and II above, that is, the policies, rules, and competencies. A forum must be established, led by the main promoter and, to the extent possible, with the

participation of everyone. In addition, NIST (2019) points to the desirability of a consensus between the leaders of the organization, particularly regarding the priorities of protection and privacy, risk tolerance, and the allocation of resources to implement and supervise the controls.

In June 2019, the World Economic Forum (WEF) created the G-20 Global Smart Cities Alliance on Technology. It groups together all municipal, regional, and national governments, private sector partners, and civil society to collect and analyze successful and ethical policies for smart cities. A roadmap and a policy of governance have already been developed (WEF, 2020, 2021). The LAC cities of Bogota, Brasilia, Buenos Aires, Cordoba (Argentina), Medellin, Mexico City, and San José all participated.

The majority of the 37 smart city pioneers (28 out of 37) of the G-20 Global Smart Cities Alliance have cyber responsibility policies. One-third have appointed a senior civil servant for this area (13 out of 28 cities) and governance plans are reviewed annually in 15 cases. Likewise, half of the cities maintain an updated inventory (18 out of 28). The IT function is not always informed of the deployment of new technologies (11 out of 28) (WEF, 2021: 20).

Mario Gogh

2.3
Institutionalize Cybersecurity

The institutionalization of cybersecurity refers to how to integrate and organize entities, resources, and information flows, with clear competencies and participation of stakeholders.

According to the IDB, one of the four elements of the smart city infrastructure (Bouskela et al., 2016) is the Integrated Operation and Control Center (IOCC), which is customary for cities of more than 200,000 inhabitants. The IOCC consists of the technological structure (computers, applications systems, and digital system monitoring), the physical infrastructure (operations rooms, crisis management rooms, etc.), the infrastructure of processes, and the staff and the representatives of various public agencies and service providers, with a collaborative and comprehensive approach to the issues to be addressed in what should be the nerve center of the smart city. Such centers are responsible for processing and analyzing the city data to inform intelligent decision-making. In some cities, they emerge from the sectors initially responsible for establishing the smart city, such as mobility, security, and emergency response, and that have gone on to integrate other objectives and functions, such as the areas of data management and intelligence.

Whether or not there is an IOCC, every city must have a security operations center (SOC). This is the main supervisory agency that monitors security information in real time and for this purpose analyzes any incident that occurs in the activity of networks, servers, applications, databases, webs, and other systems. The SOC is also a system of fluid cooperation in which information is shared among multiple stakeholders, including suppliers and commercial operators of the different services providers. The SOC integrates and shares, if there is one, with the Computer Security Incident Response Team (CSIRT) or the Computer Emergency Response Team (CERT), which prepare, coordinate, and respond to computer security incidents and emergencies. **According to each city's possibilities, the objective should be to integrate technology, processes, staff, and service provider representatives in a single center. This would permit the monitoring of security incidents in real time and allow information to be shared among all parties.**

As an example from outside the region, starting in 2013, and especially with its upcoming Expo 2020 in mind, Dubai became a world leader not only in technological innovation, but also in designed infrastructure and strategic security. In 2014, the Dubai Centre for E-Security[12] was created. It has a cybersecurity office in each of the 133 government and quasi-government entities. Furthermore, the Office of the Director General reviews its cybersecurity governance framework annually, and the Center of Security evaluates it (Efthymiopoulos, 2016). Although this is a national structure, this model can inspire regional projects and major cities.

12. See https://www.desc.gov.ae/about-us/#statement.

Yiran Ding

2.3.1

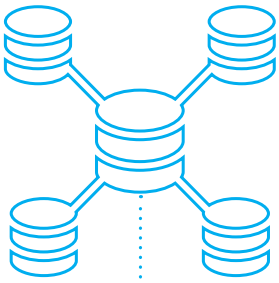
Appoint a Person Responsible for Cybersecurity

The Chief Information Security Officer (CISO) is the director of information security, an executive role that aligns information security with business objectives and ensures that the organization is protected. The Chief Information Officer (CIO) is the director of IT and is responsible for aligning ICTs with organizational strategies (INCIBE, 2016).

There is an international consensus around concentrating as many of the city's cybersecurity responsibilities as possible in the role of a senior civil servant, which may be interpreted as the CISO (G-20 Global Smart Cities Alliance, 2021; WEF, 2020). However, in some cases, CISOs lack effective and direct control. If a concentrated model is impossible, a shared responsibility model is proposed between a central information technology (IT) team, in this case the CIO, the smart city department of operations, and the office of the CISO. In Japan, the responsibility can be shared among various senior civil servants, as long as white spaces with no clear responsibilities are avoided (MIAC, 2020). In such cases there must be strong cooperation and coordination between the departments, the CISO, and the CIO. New America, Cohen, and Nussbaum (2018) warn of the pitfalls of concentrating cybersecurity in a single person or institution, especially due to inherited systems and organizations and to the difficulties inherent in merging departments and services. In any case, they underscore the advisability of having an empowered cybersecurity structure or a cybersecurity coordinator or advisor situated above the existing entities to establish priorities and coordinate or direct efforts.

Whether a small cybersecurity team should be set up, led by the CISO, a data protection officer (DPO), an expert in penetration testing and the support team, according to the activities identified for cybersecurity capabilities, is a matter of debate. The CISO should coordinate with the organization's CIO. For this purpose, a cybersecurity committee should be established. It could have a local version for the entity and another at the sector level. Generic competencies (soft skills) and cybersecurity capabilities (hard skills) should be defined for each role and profiles established.

Some cities do not have a CISO or a CIO; at most, there may be a person responsible for technology. In such a case, this person's responsibilities should be concentrated and clearly defined. Although it is better for the city to have its own internal staff, the specialized services of a CISO can sometimes be outsourced, as happens with data protection delegates or officers in many cities (AEPD, 2018).

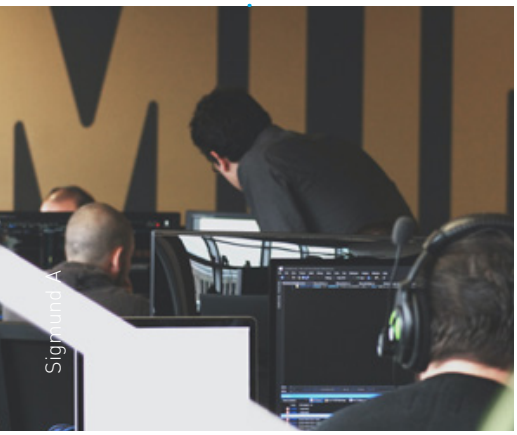


2.3.2

Determine the Functions of the Person Responsible for Cybersecurity

This senior civil servant or CISO is **responsible for ensuring that all cybersecurity measures are complied with, specifically those performed by technical staff**, and that all applicable standards and regulations are observed. This person is responsible for accountability and is authorized to execute cybersecurity throughout the entire IT and operational technology (OT) infrastructure (users, devices, networks, data, and applications). They must have a direct connection with the highest city authorities and either be a member of the city hall's senior leadership team or be directly answerable to it. The main functions assumed by the CISO are the critical responsibilities (G-20 Global Smart Cities Alliance, 2021), which can be seen in Section 4.3 of this guide.

Additionally, also reporting to the CISO, there will be a specific person responsible for networks and applications security, monitoring assets, overseeing training in data security and risk management. These tasks should be carried out at least annually, including performing audits or appointing third parties; establishing a risk evaluation policy and investigating third parties with whom activities are subcontracted and with responsibility for ensuring that citizens have access to educational materials on basic cybersecurity topics (G-20 Global Smart Cities Alliance, 2021).



2.3.3

Establish Mechanisms to Share Information on Cyber Threats among Stakeholders

Public and privates actors must share information about cybersecurity and any incidents that have occurred, with trust and in confidence, by establishing structures and points of contact and cooperation.

ENISA (2015) states that transversal and proactive exchange of information about threats and incidents is essential for uncovering threats and delivering coordinated responses. Trust among all parties concerned is also indispensable for avoiding reputational costs.


Bermix

For this purpose, anonymization and confidentiality models may be useful. In general, however, there is no reference architecture in smart cities for data exchange. For this reason, NIST (2019) indicates that consensus is needed, alongside the modification of existing structures and processes, as well as of shared services. All stakeholders must establish a point of contact in the event of an emergency situation. In the case of service providers and suppliers, contracts must specify and give details of information to be managed, and must stress the need for responsibility and communication among parties.

The city must impose or prepare channels of communication for reporting cybersecurity incidents among the different areas or services of the city itself, as well as with all external suppliers and service providers.

As part of their responsibilities, city leaders and managers should:

- **Define** a point of contact with respect to incidents.
- **Communicate** confidentiality requirements for the technical and technological levels as well as for service providers if they provide information.
- **Include** obligations to report incidents in service providers' contracts.
- **Conduct** simulations with small teams made up from different areas or urban services, as well as service providers or operators, in order to build trust and willingness to share information.
- **Establish** communication with people responsible at the higher regional and national levels.

There is no single model to follow. The public and private sectors have created cybersecurity information exchange systems. New America, Cohen, and Nussbaum (2018) offer the best cybersecurity governance practices for the smart city and highlight in particular the case of the Arizona Cyber Threat Response Alliance (ACTRA), the New Jersey Cybersecurity and Communications Integration Cell NJCCIC, a bureaucratic superstructure and common space providing a point of contact and coordination, as well as the Office of Cybersecurity (OCS) model, part of Washington Technology Solutions (WaTech), which is responsible for military and emergency management.

2.4
Integrate Confidential and Personal Data Security

2.4.1
Data Management

Cities are increasingly obtaining utility from big data, via its capture, compilation, storage, and analysis, and are extracting value for decision-making and service provision. All of the city's information and data must be protected, although this should be done according to its critical nature and level of risk. **Critical data must therefore be identified and evaluated, as well as any data particularly confidential for the city.** Cities must be aware of applicable regulations as well as the possible value of the data according to its relationship to the city's assets, strategies, interests, functions, and operations. It should also be established whether a data breach can cause direct harm to citizens, economic losses, reputational damage, or protests. For such identification and evaluation purposes, the technical and administrative levels **can use different resources**, such as the NIST (2008), the CCN (2020), or the OAS (2019). Thereafter, cybersecurity measures will be applied to the data in accordance with the value and level of risk.

It is now worth focusing especially on personal and in particular protected data. Much of the information managed by the city, in principle, is not personal, in the sense that it cannot be linked to specific individuals. However, **data that are indeed personal are being increasingly generated on a massive scale**. This is due to the trend toward the personalization of services and 360º views and, also, to sensorization and the growing employment of city apps linked to mobile devices. Geolocation data, so common in the smart city, are especially sensitive, while greater protection should be provided for data related to political or trade union meetings and demonstrations, medical or religious centers, or patterns of behavior linked to people's sex lives, and so on (AEPD, 2020b; Article 29 Group, 2011).

If the data managed by the city can be linked to particular citizens, then these are personal data and therefore subject to wide-ranging and rigorous data protection regulations. The guarantees and the security requirements will be greater still if the data are also particularly protected for racial, ideological, trade union, health, genetic, sexual, or biometric identification reasons, or refer to crimes and sanctions.

The principle of proactive responsibility should be followed when it comes to personal data: any city that manages personal data will have to comply with an entire series of obligations and be able to demonstrate that it has complied with them. Likewise, the city's data management processes and procedures must follow the rules of privacy by design and by default. Under the principle of minimization, from the very first moment, the city must use the absolute minimum quantity of data possible and for the least possible time. This goes against massive data extraction and exploitation, which is the very essence of the smart city. Minimization sets a limit on georeferencing smartphones, or on the sensors and apps of the city or its service providers. Furthermore, it is essential to carry out periodical data cleansing to avoid accumulating data that does not correspond to legitimate aims or is disproportionate. Fixed periods must be established for conserving data according to purposes, sensitivity, and risks (AEPD, 2017: 12, 17). Once this period has elapsed, data must no longer be used by the city and must remain in an encrypted state and of restricted access. Whenever the applicable legislation (on archives, transparency, administrative or criminal responsibilities, etc.) so permits, the data must be finally destroyed. If possible, any copies of the data must be automated.

Santander is one of the leading smart cities in Spain (for example, in terms of street lighting and waste collection). It is also noteworthy for applying privacy and security standards from the design stage. The person responsible for cybersecurity and local firms participate in defining smart city initiatives before their implementation and in determining the measures to apply. Thus, for example, following the COVID-19 pandemic, a comprehensive system for monitoring the affluence of people in municipal buildings has been established.

In accordance with the principle of loyalty, the city may only manage data for the purposes approved from the legal and legitimate point of view. In general, data may be managed for administrative purposes, tax management, social, education or health service provision, and so on. What is not so clear is whether the smart city is allowed to reuse those data to improve these or other services, to evaluate, monitor, control, or decide public policies, and so on. Often the laws are insufficiently clear with respect to the use of personal data by cities or, specifically, for smart city projects (as a positive exception, the UK

Digital Economy Act of 2017, Sec. 35, is worth mentioning).[13] **Care must be taken to ensure that the project or treatment of personal data enjoys sufficient legal backing.**

In all massive data treatment undertaken by a city, and before deployment of a smart city project, it is obligatory to carry out a risk analysis and very possibly a complete study of its impact on data protection (Art. 35 of the General Regulation of Data Protection [Reglamento General de Protección de Datos, or RGPD];[14] AAEPD, 2018; AEPD, 2020a: 22). Therefore, the information and the volume of data to be managed must be evaluated, alongside their sources and conservation; the risks and impacts must be assessed and, according to these, the security and organizational measures to be implemented. The AEPD (2021) explains how to do this in its *Guide to Impact Evaluations (Guía de Evaluaciones de Impacto)*. **In view of the close connection and the similarities that exist in these matters, compliance with data protection must be closely linked to cybersecurity actions.**

Data exploitation by the city has become increasingly intensive and has incorporated successive layers of artificial intelligence. Therefore, precautions and mandatory auditing must be considered. In essence, there must be quality management of the entry data and the data used to train the system; bias controls, guarantees of the robustness of the artificial intelligence system; verification that records or system logs are created that prove system operation and register incidents, monitoring of traceability, transparency, explainability and recurrence, as well as constant auditing and evaluation. In this area, the AEPD guides to artificial intelligence may be consulted (2020a and 2021).

The creation, in 2020, of the Algorithms Register[15] of the city of Amsterdam is worth mentioning. It permits a high degree of citizen transparency with regard to the use of artificial intelligence in the smart city. The register presents general and also technical descriptions and offers the possibility of participating in initiatives.

Likewise, on June 30, 2021, Barcelona, London, and Amsterdam created the Global Observatory of Artificial Intelligence to monitor the ethical application of artificial intelligence in cities. UN-Habitat and the Barcelona Center of International Affairs (Centro de Asuntos Internacionales de Barcelona, or CIDOB) all collaborate in this initiative.

13. See https://www.legislation.gov.uk/ukpga/2017/30/section/35.
14. See https://www.boe.es/doue/2016/119/L00001-00088.pdf.
15. See https://algoritmeregister.amsterdam.nl/en/ai-register/?s=08.

Omar Prestwich

"The essence of cybersecurity is thus laid out: knowledge and understanding of the environment, planning, prevention and surveillance, collaboration and cooperation, and ongoing education and training."

2.4.2
Anonymization and Pseudonymization: Essential Strategic and Security Measures Enabling the City to Manage Data

As mentioned above, it is necessary to identify, evaluate, and apply to the data and information the security measures corresponding to the level of risk. In any case, it is clear that **many difficulties in complying with data protection regulations can be resolved if the data can be successfully disassociated from the people who create them**. This is a concern that the IDB has already identified for managers in all cities (Cerdeira et al., 2020: 28). Therefore, the data must be anonymized in accordance with the standards established by the data protection authorities (AEPD, 2019a; ICO, n.d.). If the data are entirely anonymized, then there will be no need to apply data regulations, and the city and its service providers can use them freely and with fewer security measures. Nonetheless, total anonymization is becoming increasingly difficult to achieve, as there are more and better technologies to reverse anonymization and re-identify the people.

An essential strategy is known as pseudoanonymization. This consists of **anonymizing the data as far as possible** and enabling city services or service providers and firms to manage the data and exploit and extract its value without identifying the person. At the same time, non-personal data (NPD) remain isolated from the city departments or agencies that do have re-identification capacity. Thus, in the event of breaches or leaks, only non-personal data will be accessed. Furthermore, **pseudonymization makes it legally much easier for the city to exploit its citizens' data for smart city-related purposes, statistics and research**, and so on.

2.5

Integrate Service Providers and Cybersecurity

Cybersecurity must be incorporated into the choice, procurement, and management of suppliers and service providers. For this purpose, certain procurement guidelines such as those recently set out for health service procurement (ENISA, 2020) may be followed.


Lagos Techie

In accordance with NIST (2019), **this permits the city to maintain control and dictate risk management requirements, thus preventing service providers from imposing their own requirements on the city**. However, Ranchordás and Goanta (2020) warn that cities often end up acquiescing to the conditions imposed by the big platforms, in detriment to common values and interests, cybersecurity and citizen rights. In such a situation, cities should share information about suppliers and service providers and establish standard clauses and contracts. Soare and Burton (2020) consider it "paradoxical" that public procurement still fails to focus sufficiently on cybersecurity. The CISO or senior civil servant has, among their essential responsibilities, to make decisions on the cybersecurity of any significant investment in IT and operational technology products or services acquired by the city. Shacklett (2019) underscores that the regulations relative to IT security must be met to the letter. Manufacturers and providers must follow security approaches starting from the design of the technologies and services acquired, such as those established in general by ENISA (2014): security by design, least privilege (permit restrictions), strong authentication, asset protection, supply chain security, document transparency, quality management, service continuity, and restricted use of data.

These guidelines should be followed in specifications and procurement:

- Guarantee cybersecurity requirements at the service provision level in a service level agreement (SLA) (WEF, 2021). Likewise, information leaks by sub-contractors must be avoided (MIAC, 2020).
- Establish a specific incident response plan (Cerrudo, Asbini, and Russell, 2015). Support for incident response must also be included 24/7/365.
- Establish the tests to which the system will be submitted and determine the certification requirements for third parties. Audits and searches must also be permitted, and the delivery of security audit reports should be agreed on an annual basis.

- Define who will conduct monitoring and control of compliance with the cybersecurity obligations to be met by third parties and subcontractors, and how it will be conducted.
- Define what information is to be shared and what the functions and responsibilities will be, and so on (MIAC, 2020). An effective system for reporting and correcting vulnerabilities that involves service providers must be described in detail (ENISA, 2015). Interoperability must therefore be guaranteed.
- Enter into confidentiality agreements that permit information about incidents to be shared without the need for public disclosure (NIST, 2019).

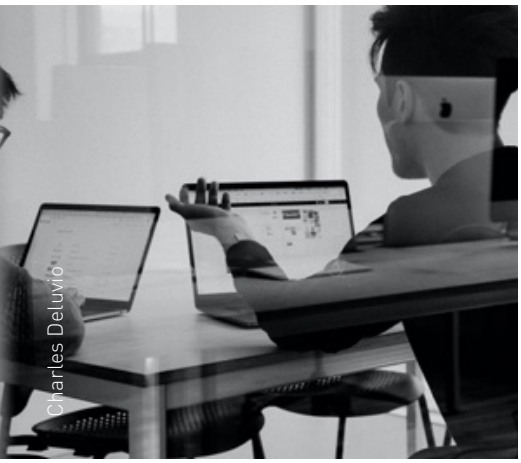
Forrest (2019) adds some **elements to take into account when choosing a service provider**, such as whether this could lead to negative publicity or mistrust of the contractors. From the financial point of view, it is worth considering whether it is profitable, whether there are other large customers and what the exit strategy is. It might be useful to seek help from specialized firms to examine the profile of service providers and their risks. Notwithstanding all of the above-mentioned precautions, in the case of emerging service providers in innovation and pilot projects, it might be sensible to make the demands less rigorous.

Data protection regulations often stipulate that contracts must include certain contents, and some aspects are directly related with security measures. Thus, contracts between the city and the firm must regulate the relations between the person responsible (the city) and the service provider (contractor) and give detailed instructions for the latter, the duty of confidentiality, the security measures applicable, subcontracting possibilities, the rights of stakeholders, collaboration obligations, the storage or elimination of data after the service, as well as the means at the city's disposal to ensure that such conditions are met. For this purpose, the model and the Procurement Directives of the AEPD (2019) can be followed. If firms use the data for other purposes in their own interest, this must be clearly stipulated in the contract, and the firm will thereby become responsible or co-responsible in terms of data protection.

2.6
Train, Communicate, and Raise Awareness about Cybersecurity

Cybersecurity requires training, communication, and awareness-raising. The person responsible at the senior level or city manager must therefore design the training plans, as well as plans for aware-raising and communication.

2.6.1
Establish Training Plans


Charles Deluvio

According to Stuart Chontos-Gilchrist, of E3 Technology, "firms are recognizing that people, more often than machines, are the ones that cause security breaches."[16] Hackers always seek out the weakest link and, in general, the vectors of attack include not only technology, but also employees (ENISA, 2015, Section 5.1). The human factor means everything and the human threats are the most significant (NCSC, 2021). Managers and staff must be aware, trained and up to speed to act correctly (Bouskela et al., 2016: 45; Shacklett, 2019).

The senior civil servant responsible for cybersecurity is also in charge of the **ongoing training of employees, which must be well planned and provided with sufficient resources**. As Stilgherrian (2019) points out, training in security is worthless if it fails to change behaviors and if there is no commitment. Commitment and cultural change must be actively sought. It is therefore essential, in the first place, to train staff in matters of personal cybersecurity (networks, family, household, minors, abuse, etc.). It will thereafter be much easier to involve them in the organization's cybersecurity problems and in employing best practices, such as, for example, not repeating or sharing passwords, updating them frequently, not responding to suspicious messages, not sending information through unsafe channels, not using public equipment for private aims (and vice versa) and not installing unauthorized programs on their devices, and so on. It is worth considering encouraging staff to share experiences and security fears with their colleagues (see the Australian Government's "It's time to #askoutloud about cyber safety, Stay Smart Online."[17]

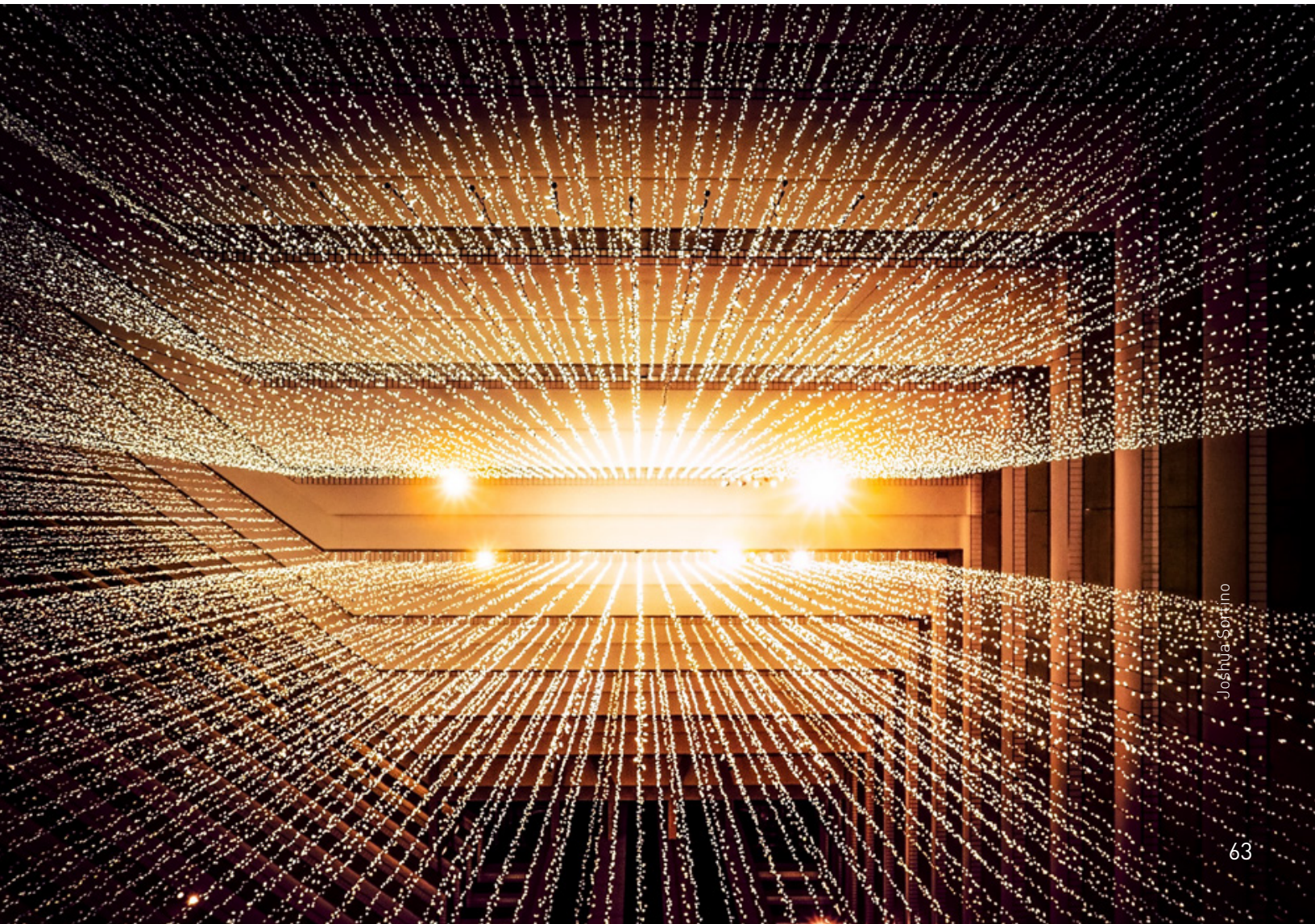
16. See https://www.e3security.com/about.

17. See https://www.acic.gov.au/media-centre/media-releases-and-statements/its-time-askoutloud-about-cyber-safety.

2.6.2
Establish Communication Plans

The people responsible for security have to clearly explain cybersecurity technologies, policies and practices in a simple language that can be understood by mayors, managers and city executives not familiar with the technology field. Management must understand why it is enacting regulations or policies, or making significant investments. If managers themselves do not understand, they will be unable to explain or defend it. And, obviously, without the need for a security problem to happen to make everything very clear.

Downstream communication is equally important. **Cybersecurity policies and regulations tend to be dry, complex, and not at all inspiring for employees.** Investment must be made in good communication of such policies and regulations and, as previously mentioned, the personnel must be convinced to take security concerns seriously.


Joshua Sortino

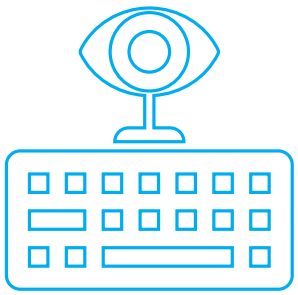
2.7

Make Cybersecurity Financing and Insurance Available

A smart city requires financial security (Townsend and Zambrano-Barragán, 2019: 39) and **cybersecurity needs a budget, which, if not provided in time, becomes increasingly expensive. The social, political, and economic costs and the undermining of trust caused by failing to invest in time can be enormous**. ENISA (2015) points out that cybersecurity knowledge and spending are relatively low compared to the impacts of potential attacks (such as those mentioned in Section 1.4.3). Therefore, its Recommendation no. 7 is that operators, service providers, and the city hall should allocate a larger cybersecurity budget, in particular to raise awareness and offer training to all staff and senior management, as well as helping them to develop knowledge and to facilitate acceptance of solutions from third parties that comply with security requirements.

Resource demands should be planned, while reviews of the system design, testing, active supervision of network traffic, insurance, and the technical, contractual, and legal costs associated with repairing and recovering from a security breach should also be calculated. Obsolete and outdated systems seriously jeopardize cybersecurity. Soare and Burton (2020) show that the prolonged periods of budget austerity introduced since 2010 have had negative effects and that the economic recession derived from the COVID-19 crisis can make the situation worse.

In the initial phases, the city must also weigh contracting **cybersecurity insurance** and, obviously, integrating it with its budgets. According to a Wall Street Journal survey, most of the 25 largest cities in the United States either already have cybersecurity insurance or are considering acquiring it (NIST, 2019). Such insurance policies can provide cover for any harm (even reputational) produced by an attack. Coverage may include services to repair damages, recover data and equipment, protect identities, and respond to claims by third parties. Likewise, **if the city has a cybersecurity insurance policy, this may generate positive preventive dynamics.** Insurance normally covers some prevention services and consultancies on regulatory compliance.



Furthermore, there are preventive cybersecurity obligations. Taking out insurance, then, as well as limiting damage in the event of attacks, provides encouragement to carry out regular evaluations, hold training courses, update equipment, make back-up copies, and other such measures.

The previous sections have detailed the resources, recommendations, and the best practices to enable cities to respond to cyber threats. The first step is to take into account the complexity of the ecosystem and its numerous actors. A set of appropriate policies, rules, agencies, responsibilities, and formulas of governance has been described, including a good connection with regional and national levels of cybersecurity. Cities manages much personal and confidential data and should analyze risks and implement security measures accordingly. Data anonymization and pseudononymization is particularly recommended as a basic legal and security strategy. The importance of sharing information among parties has been underlined, alongside the key elements for the procurement and selection of service providers and suppliers. In any event, awareness-raising and training for the people responsible and city staff continues to represent one of the best possible investments. All of this requires resources and budgets. This roadmap, depicted in Figure 2.2, is suitable for all types of cities: there is no need to wait until tomorrow before putting it into practice.

Stem T4L

Figure 2.2.

Roadmap of Urban Cybersecurity Responsibilities

Government leaders

1. Define the vision and objectives of the cybersecurity initiative. Establish the sector or sectors within its scope.
2. Establish the necessary rules and policies: agreements, ordinances, decrees, resolutions, or administrative acts, aligned with the regional and national cyber strategy. Incorporate standards into the rules.
3. Build the institutions needed to materialize cybersecurity. Identify the person or people responsible and their functions. Determine the coordination scheme for dealing with incidents.
4. Identify and evaluate the critical data, as well as those especially confidential for the city.
5. Establish a municipal management team to integrate cybersecurity into the process of procuring, managing and contracting service providers.
6. Establish a municipal management team to drive forward the training and communication processes.
7. Establish a municipal management team to lead the financial and insurance processes.

Municipal leaders

1. Working with the technical team, identify the services that need protection. Define the plans, programs, and projects aligned with the policies. Identify the actors involved.
2. Create the processes for compliance with, and materialization of, rules and policies.
3. Establish the internal processes and procedures to build institutions in the sector.
4. Establish the internal processes and procedures for identifying and evaluating the critical data, as well as data that are particularly sensitive for the city.
5. Integrate cybersecurity into the process of procuring, managing, and contracting service providers.
6. Establish a training and communication plan for the sector.
7. Establish a financial and insurance plan for the sector.

IT staff

1. Identify the information associated with the support services and assets to be protected.
2. Comply with and execute the rules and policies deployed for the cybersecurity function. Identify the cybersecurity model to follow.
3. Within the framework of the cybersecurity model, define and implement the capabilities. For this purpose, the technological and information processes must be integrated into institutions.
4. Identify and evaluate the critical data, as well as data that are particularly sensitive for the city.
5. Establish the basic security requirements to be incorporated into a safe technology product and service procurement process.
6. Execute and communicate the training plan.
7. Execute the financial plan in accordance with the agreed roadmap and the resources allocated.

Source: Authors' elaboration (2021).
Note: The responsibilities presented in this graph must be articulated with the responsibilities that are established for the intermediate level personnel between municipal leaders and municipal managers, and, in turn, between these and the cybersecurity and IT personnel.

3 Cybersecurity Rules for Staff at the Strategic, Tactical, Operational, and Technical Levels

Ruslan Bardash

"Cybersecurity is in the hands of the city's administrators, officials, and employees, who carry out specific actions to execute policies, plans, and programs and are familiar with each specific area of the city."

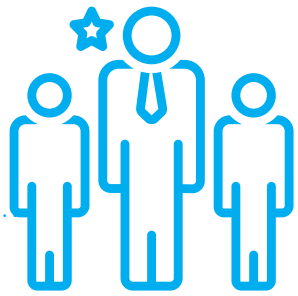
3.1
Rules for Mayors and Senior Leaders

Government Leaders — Strategic Level

Cybersecurity depends on general executive management, as well as on vision, leadership, strategic action, and goal setting, alongside policymaking and resource management. With this in mind, the following recommendations are worth highlighting:

1. **Make political agreements** with the different sectors. Cybersecurity is a policy for the city as a whole and goes beyond an electoral mandate; it requires consensus, resources, and a medium and long-term vision. This will facilitate the prioritization and allocation of the required resources in this area.
2. **Send political messages** aimed at raising awareness among both civil servants and citizens to achieve political support. It is not necessary to suffer a cyberattack to understand the negative impacts it can have.
3. **Express support for cybersecurity policy** in a single voice. Make the stakeholders involved adopt strategies, policies, rules, and clear competencies in terms of cybersecurity. Exercising leadership, the mayor or the person responsible can grant legitimacy and strengthen actions to unite divergent areas within the public and private sectors.
4. **Build institutions** and consider creating an area of coordination and control centers with well-defined competencies in the field of cybersecurity. Provide them with resources and, in particular, support their integration and cooperation.
5. **Encourage awareness-raising**, ongoing formation, and training in cybersecurity for managers and staff, and ensure that there are similar campaigns for citizens. Cybersecurity is everyone's responsibility. Make sure that the rules, policies, and plans do not get stuck at the starting gate, and promote testing, simulations, and continuous evaluation.
6. **Involve the city's private sector** service providers and suppliers. Maintain coordination and trust-building mechanisms. Ensure that city hall establishes the terms of procurement and that these include cybersecurity, even in start-ups and small- and medium-sized enterprises (SMEs), through policies, plans and financing.
7. **Stimulate the update and replacement of obsolete technology** assets and the procurement of goods and services with security by design and by default, which automate cybersecurity and employ emerging technologies.
8. **Ensure that cybersecurity is one of the elements to be evaluated** in city, especially smart city, policies.
9. **Employ financial planning mechanisms** that help maintain projects over the short, medium and long term. Remember that cybersecurity needs resources and financing.
10. **Encourage the city's participation in national cybersecurity networks** for cities. Local cybersecurity programs must be aligned with metropolitan and national strategies. Pay special attention to the resources on offer at the national, federal and even international level.

3.2
Rules for Municipal Officials and Employees



Municipal Management — Tactical Level

Notwithstanding strategic decisions, cybersecurity is in the hands of the city's administrators, officials, and employees, who carry out specific actions to execute policies, plans, and programs and are familiar with each specific area of the city. The following recommendations are addressed to them, according to their position and responsibilities:

1. **Cybersecurity starts with every individual,** with their own computer and mobile phone. Identify the technology and the infrastructure that needs protection from the cyber perspective, as well as the actors involved.
2. **Get to know** and to understand the threats to which one is exposed in cyberspace. To the extent possible, carry out a self-evaluation or assessment of the level of maturity in cybersecurity.
3. **Find out what specific cybersecurity actions,** strategies, rules, policies, and procedures are in place in the city and what your competencies are. If it is your responsibility, make sure your subordinates are also aware.
4. **Do not leave policies and rules on the shelf.** Put your own responsibilities to the test, take part in simulations, and adopt the processes and procedures. If a security failure is detected in the city hall or in the service provider, this must be communicated to the competent agency, even confidentially.
5. **Participate in training** and refresher programs to better carry out cybersecurity responsibilities.
6. **Communicate policies** and directives effectively so that everyone can take them on board. Share cybersecurity experiences with colleagues, other areas, and other local governments.
7. **Find out whether the material**, human, financial, and technical resources needed to meet cybersecurity responsibilities are available. If insufficient, plan and request that the necessary resources be provided.
8. **If applicable, plan and structure human resources,** recruiting qualified staff for cybersecurity and new technologies.
9. **To the extent possible, seek cooperation with private service providers and suppliers**, interact with them, and create a climate of trust in which critical cybersecurity information can be shared.
10. **Ensure that contracts with service providers include obligations,** documentation, and adequate customer service responses; also make sure that suppliers understand the security requirements and verify their compliance.

3.3
Rules for Technical Cybersecurity and IT Staff

Operational Level

The following recommendations are addressed to the people responsible for, and familiar with, the technologies and systems needed to protect the city. These are the staff who follow the strategies and tactics planned by the other levels and propose the technical and training directives and the procedures for managing, identifying, protecting, detecting, responding to and recovering from incidents. The IT staff are often responsible for cybersecurity, although sometimes there maybe other experts with specific responsibilities in the matter. The recommendations include the following:

1. **Identify the scope,** the services and systems to be protected, especially those for which you are responsible, and be very clear about the agencies and actors responsible for them.
2. **Know the guidelines,** strategies, policies, rules, and best practices defined in the city and make them operational in the systems for which you are responsible.
3. **Participate in and contribute to cybersecurity evaluation,** management, and planning as a continuous process.
4. **Identify the specific cybersecurity entities** and responsibilities in the entity in which you work, and know what one another's responsibilities are in the event of incidents and responses to them.
5. **Carry out a self-evaluation** or assessment process of the city's level of capability maturity according to the tools at your disposal, and then calculate the capabilities and resources needed.
6. **As far as your contractual responsibilities allow, plan and determine the specific steps needed** to achieve the objectives.
7. **Protect and implement identification,** authentication, and access control systems, as well as mechanisms for monitoring and detecting anomalies and responding to incidents.
8. **If within your capabilities, ensure that procurement of technology goods and services by the city includes security and privacy** by design and by default. Keep up to date with the new methods and tools used by hackers. Update and improve the state of hardware and software. If possible, opt for automated systems for detecting and responding to threats. If within the scope of your responsibilities, take a leading role and create dynamic or active security teams to preempt attacks.
9. **Establish the professional profiles** of the team responsible for the cybersecurity function, based on the roles defined in the processes and procedures.
10. **Integrate privacy and data protection policies** with those of cybersecurity.

4 Technical Capabilities for Providing Cybersecurity to the City

Augusto Navarro

"One of the commitments to be assumed is compliance with the rules, policies, and guidelines deployed for the cybersecurity function."

4 Technical Capabilities for Providing Cybersecurity to the City

The reader of this guide will have already understood the dangers, cyber threats, actors, motivations, and impact that cyberattacks can have on cities and therefore the need to take urban cybersecurity seriously starting now. Readers thus already have the resources, best practices, and recommendations that will enable them to begin the task. Nonetheless, cybersecurity also includes an inevitable technical component. This section is aimed especially at managers and staff with a technological background responsible for cybersecurity in the city. It provides a roadmap for implementing capability maturity models. One of the commitments to be assumed is compliance with the rules, policies, and guidelines deployed for the cybersecurity function (Figure 4.1).

Figure 4.1.

Guidelines for Cybersecurity and IT Staff

1. **Identify** the information associated with the support services and assets to be protected.
2. **Comply** with and execute the rules and policies deployed for the cybersecurity function. Identify the cybersecurity model to follow.
3. **Within the framework of the cybersecurity model, define** and implement the capabilities. For this purpose, the technological and information processes must be integrated into institutions.
4. **Identify** and evaluate the critical data, as well as data that are particularly sensitive for the city.
5. **Establish** the basic security requirements to be incorporated into a safe technology product and service procurement process.
6. **Execute** and communicate the training plan.
7. **Execute** the financial plan in accordance with the agreed roadmap and the resources allocated.

Source: Authors' elaboration (2021).

The essential objective of the roadmap is to implement and strengthen capabilities, thereby enabling initiatives to be put into operation over the medium and long term. Capabilities are defined based on the cybersecurity maturity model chosen (Table 4.1). According to their needs, technical staff can opt for one of the different existing maturity models.

Table 4.1.

Cybersecurity Maturity Models for Organizations

Acronym	Name	Proposed by	Levels of Maturity
CCSMM	Community Cybersecurity Maturity Model	White	5
COBIT	Control Objectives for Information and Related Technologies	ISACA	5
CSF-NIST	Cybersecurity Framework	NIST	5
C2M2	Cybersecurity Capability Maturity Model	Curtis	4
ISMS	Information Security Management System—ISO/IEC 27001	ISO/IEC	5
ISM3	Information Security Management System—Maturity Model	ISM3	5
-	Cybersecurity Capability Maturity Model of the National Initiative for Cybersecurity Education (NICE)	US DHS	3
RMM	Resilience Management Model	CERT	4
SSE-CMM	System Security Engineering—Capability Maturity Model	NSA	5

Source: Adapted from Rea-Guaman et al. (2017).

The development and implementation of technical capabilities can be gathered into a "cybersecurity function" that comprises **management** (process reengineering and definition of key functions); staff formation and training, and change management; **technical activities** (information or software systems and the infrastructure or hardware that supports them); and, finally, **information management** (that connects the processes with IT, digital technologies, and emerging technologies). The IT staff are responsible for this cybersecurity function, which means that it should follow the three steps described below: self-evaluation of capabilities, identification of capabilities that need developing, and operation of the cybersecurity function.

4.1
Steps of the Cybersecurity Function

As already mentioned, the cybersecurity function is developed in three steps (see Figure 4.2).

Figure 4.2.

Steps to Follow to Implement the Cybersecurity Function

1. **Self-evaluation of capabilities**
2. **Identification of capabilities to be developed**
3. **Operation of the cybersecurity function**

Source: Authors' elaboration (2021).

The first step in implementing the cybersecurity function is conducting a self-evaluation process or assessment of the level of capability maturity, in accordance with the instruments of the model chosen and information about the services and support assets to be protected. In the case of this guide, the self-assessment is included via the link **www.iadb.org/cibereval**, which takes as a point of reference the NIST cybersecurity model, one of the most commonly used. However, any of the models or practices adopted can be used or combined according to the city services that need protection.

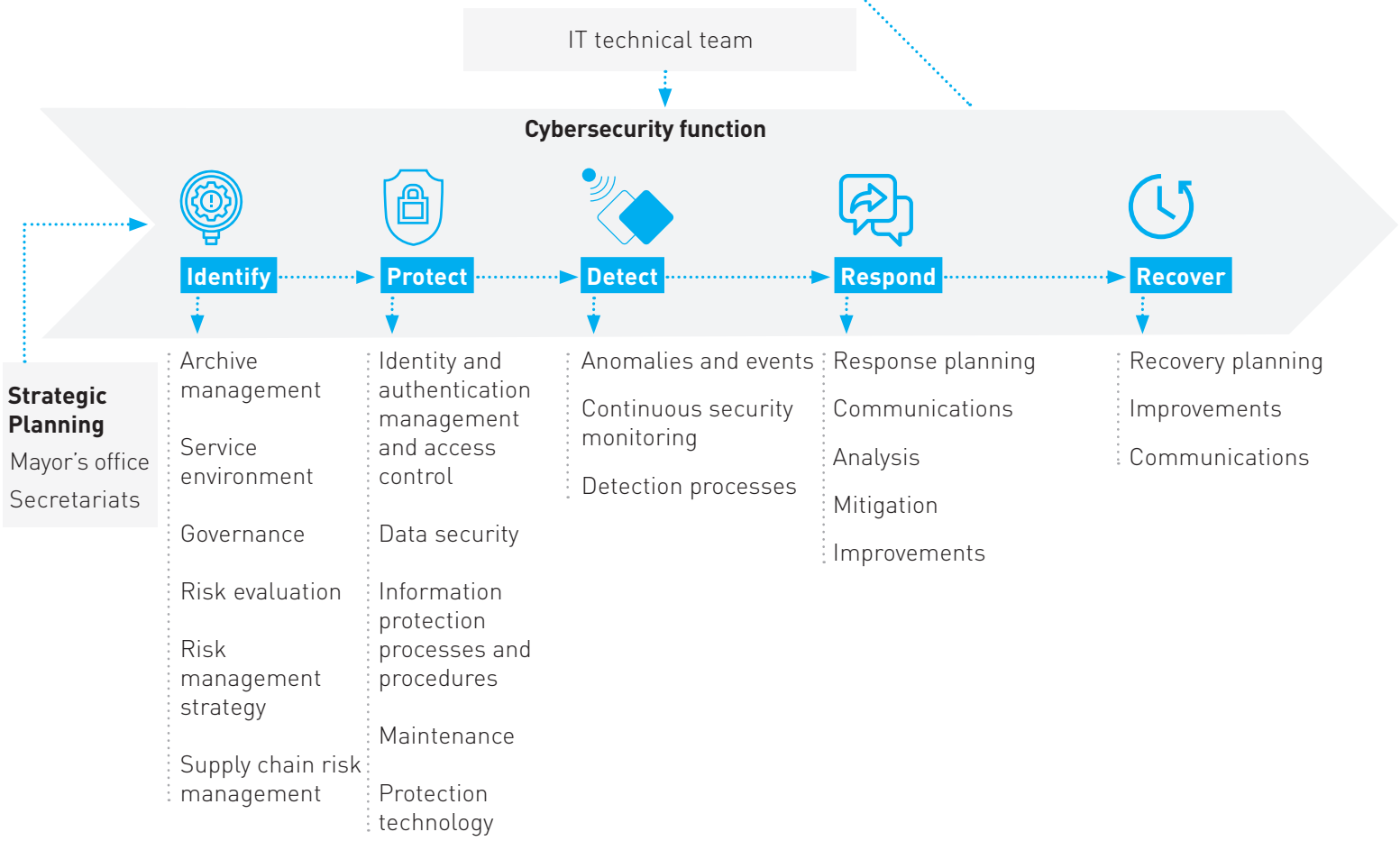
Among other objectives, the self-evaluation process seeks to determine the level of maturity based on the following questions:

1. **What activities must be carried out?**
2. **What information is used or produced in the processes?**
3. **Which people have the capabilities?**
4. **Which technology should provide support for these capabilities?**

The second step is to identify the capabilities that the cybersecurity function must develop based on the results obtained in the self-assessment. Identifying the capabilities will be linked with identifying, protecting, detecting, responding to, and recovering from any incidents that may occur in the services provided.

Figure 4.3.

Identification of Cybersecurity Capabilities



Source: Authors' elaboration (2021); Modeled on the NIST Cybersecurity Framework, using ArchiMate 3.10.

The **third step** is to put the cybersecurity function into **operation**. As an example, the NIST Cybersecurity Framework is worth mentioning. It corresponds to specific actions that point to **five capabilities**: identify, protect, detect, respond and recover, which are examined in greater detail below.

4.1.1
Identify

This capability helps to understand the context in which the city's services are delivered, the resources that support the critical functions, and the cybersecurity risks related with the provision of such services. It makes it possible to manage the cybersecurity risk to systems, people, assets, data, and capabilities. A list of the sub-capabilities that form part of this capability is presented below, in accordance with the categories proposed by the NIST, for which the financial services of a municipality are taken as an example.

Identify

- Archive management
- Service environment
- Governance
- Risk evaluation
- Risk management strategy
- Supply chain risk management

Identify:

The physical devices and systems, software platforms, and applications integrated with financial management of the city.

The hardware, devices, data, time, staff, and software, according to their classification, critical nature, and value, which are integrated with the city's financial services.

The supply chain integrated with the financial services.

The legal and regulatory requirements with respect protecting the data exchanged in the city's economic and financial transactions.

The impacts and the probability that the financial service will be affected by a computer attack.

The risk management strategy for the financial services to which support is provided.

Andy Holmes

4.1.2
Protect

This comprises the sub-capabilities that help to develop and implement adequate security measures for guaranteeing the provision of urban services. It includes the capability to limit or contain the impact of a possible cybersecurity attack.

Protect

- Identity and authentication management and access control
- Data security
- Information protection processes and procedures
- Maintenance
- Protection technology

Carry out protection activities such as the following:

Auditing the devices used.

Issuing identities, credentials, and authorizations for accessing the city's financial services.

Training the users of the city's financial services.

Using integrity testing mechanisms to verify software, firmware and information integrity.

Establishing change control processes for the configuration of systems that sustain the city's financial information.

Making and maintaining back-up copies.

Establishing and managing cyberattack response plans.

Protecting the communications and control networks.

Implementing mechanisms (for example, failsafe mode, load balancing, hot swap) to comply with resilience requirements in both normal and adverse situations.

Christina Wocin

4.1.3
Detect

Implies developing and the implementing appropriate actions to identify the occurrence of a cybersecurity incident in city services.

Detect

- Anomalies and events
- Continuous security monitoring
- Detection processes

Carry out detection activities such as the following:

Gathering information and analyzing the attacks detected to understand the objectives and methods.

Determining the impact of the attacks.

Monitoring the activity of staff, service providers, and the network to detect possible cybersecurity events.

Establishing mechanisms to identify unauthorized software, malicious code, and so on.

Approving the detection processes.

Vladimir Kudinov

4.1.4
Respond

This capability consists of developing and implementing appropriate mechanisms to take action in the event that a cybersecurity incident is detected.

Respond

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

Put into operation response actions such as the following:

Executing the response plan during or after an incident.

Reporting incidents to the authorities and in accordance with the coordination plan established by the institution.

Investigating reports from the detection systems.

Understanding the impact of the incident.

Performing forensic analysis.

Incorporating the lessons learned into the response plans.

Updating the incident response strategies.

Containing and mitigating the incidents and vulnerabilities identified.

Documenting the entire process, incorporating lessons learned, and updating the response plan.

Álvaro Reyes

4.1.5
Recover

This capability involves developing and implementing appropriate actions to maintain resilience plans and to reestablish any capability or service affected by a cybersecurity incident.

Recover

- Recovery planning
- Improvements
- Communications

Recovery actions such as the following should be carried out:

Executing the recovery plan during or after a cybersecurity incident affecting the city's financial services.

Incorporating the lessons learned into the recovery plans.

Restoring the reputation of an entity affected after the incident.

Communicating recovery activities to internal and external stakeholders, as well as to the executive and management teams.

Sammy Ayot

4.2

Technology of the Cybersecurity Function

The cybersecurity function may require different information processing services, ranging from specialized hardware and software services for penetration testing to monitoring, auditing, and forensic computer services. Automated systems should be chosen whenever possible.

IFLY:D

4.3

Functions of the Person Responsible for Cybersecurity

The person responsible in this area must fulfill the following functions:

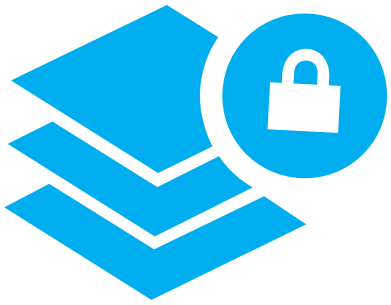
- Informing the city cybersecurity chief of all matters related to cybersecurity and communicating with the competent authorities.
- Establishing the general framework of governance and the cybersecurity policy, which must be reviewed and approved by senior leaders at least once a year.
- Enforcing the assets and equipment security policy, guaranteeing compliance with applicable regulations and supervising the annual review of information security-related documents and audit results.
- Making an inventory and having a clear vision of the technology infrastructure that needs protection. Making decisions on the cybersecurity of all products, services, and procurement and developing internal IT applications and existing operational technology.
- Executing security and privacy impact evaluations.
- Cooperating with private sector service providers and overseeing the inclusion of cybersecurity in procurement processes.
- Taking responsibility for training civil servants and carrying out annual evaluations of the same.
- Examining and recording all security incidents and adopting the necessary measures according to a specific incident and disaster response and recovery plan. This strategy should be tested at least once a year for certain systems.

5 The IDB and Cybersecurity in Cities

Zhu Hongzhi

"The IDB as a strategic partner seeks to support the region's countries to help them tackle the new challenge of urban cybersecurity."

5 The IDB and Cybersecurity in Cities



The IDB Group has developed "Vision 2025: Reinvest in the Americas" as a guide for supporting the countries of LAC in their post-pandemic recovery efforts. The Vision is based on five pillars: (i) digital transformation and faster adoption of technologies in both the public and the private sectors, (ii) strengthening the region's value chains, (iii) climate change, (iv) support for SMEs, and (v) gender equality and inclusion. The Vision seeks to drive opportunities for sustainable growth, reactivate the region's economy, promote social progress, and strengthen good governance.

For more than a decade, the IDB has accompanied the region in digital transformation. **The Digital Transformation Action Framework**[18] proposes to strengthen connectivity, public digital management, the digital transformation of social services and infrastructure, sustainable development, and the digitalization of cities, as well as digital transformation of the private sector.

Digital transformation and the use of new technologies and big data contribute to public policymaking to respond to major social challenges and to achieve the United Nations Sustainable Development Goals (SDG). The COVID-19 pandemic has accelerated the **digital transformation** of countries in the region, but **cities** face still greater challenges in guaranteeing the continuity of the provision of goods and services to citizens.

The transformation of a city into a more intelligent management model using digital technologies increases the vulnerability of assets in cyberspace.

Cybersecurity is therefore an emerging and crucial issue that concerns the region and all its cities and is acquiring growing visibility on the subnational, national, regional and world political agenda, in the context of globalization of computer systems and value chains.

18. At the time of publication of this document, the Framework was still pending approval.

Therefore, the IDB as a strategic partner seeks to support the region's countries to help them tackle the new challenge of urban cybersecurity.

The Bank has strategic partnerships with the governments that are the most advanced in digital terms, including cybersecurity; for example, Canada, Estonia, Israel, South Korea, Spain, and the United Kingdom, as well as with key partners from the academic world, the private sector and the development agencies. This allows it to have rapid access to knowledge and its exchange.

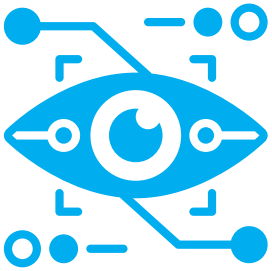

Scott Graham

Additionally, the IDB technical team collaborates with teams in beneficiary governments and supports digital transformation adapted to the reality of each country, metropolitan area, or municipality.

The Bank has a team that is dedicated to offering support to the countries of LAC in the area of cybersecurity, which is part of the Innovation in Citizen Services Division (IFD/ICS). Under the Data and Digital Government Cluster, projects are designed to strengthen cybersecurity at the national level or to strengthen cybersecurity capabilities in sectors such as transportation, health, financial services, citizen security, and digital government, among others, on which citizens depend. Furthermore, it supports public policymaking on cybersecurity, by training professionals and generating and exchanging knowledge. Among the most noteworthy studies published by the team, as already mentioned, is the *Cybersecurity Report 2020: Risks, Progress and the Way Forward in Latin America and the Caribbean*, written in collaboration with the OAS. It compiles the cybersecurity policies and best practices from around the region's countries and examines their cybersecurity capability maturity, as well as examining past breaches and opportunities for action in this field.

At the subnational level, the region's cities have recorded accelerated demographic growth in recent decades, which means that digital transformation and the adoption of technology for the provision of public goods and services have become increasingly important.

Urban cybersecurity and municipal cybersecurity have therefore rapidly evolved into a fundamental issue that must be addressed preventatively.



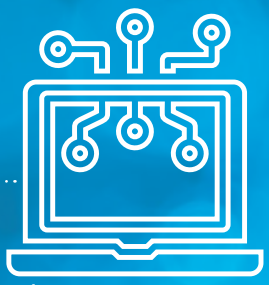
In this area, the Bank's thematic group **Smart Cities and Civic Data**, within the Housing and Urban Development Division (CDS/HUD), provides its support for the transformation of cities toward a smart cities and cybersecurity model. At the local level, cybersecurity grows in importance insofar as cities increasingly make use of technology for service provision and management of physical and digital infrastructure.

To reduce the knowledge gaps in digital transformation, the IDB has developed cybersecurity studies, pilot projects, and self-evaluation tools in sectors such as energy and health, to which the specific area of cities has now been added (https://www.iadb.org/cibereval). This tool will help discover the level of prevention and preparedness of cities to cyberattacks, as well as defining future capacity-building initiatives that the IDB can support to strengthen urban cybersecurity.

We hope that *A Cybersecurity Guide for Smart Cities* will be the starting point for a better understanding of cybersecurity, as well as its risks and potential impacts, and for sharing recommendations for transforming the region's 17,000 cities into more cybersecure, smarter cities.

Sung Jin Cho

Conclusions



Cyber threats have reached the gates of all cities, seeking to exploit technological and human vulnerabilities. Total cybersecurity does not exist, but there are many actions that can be put in place in every city to achieve the greatest possible protection. While it is true that this requires resources, as in everything else in life, what is really needed is clear willingness and commitment by city managers and staff, as well as from the private firms that participate in this area.

This guide makes it possible to understand the problem and to begin to tackle it at the same time, depending on the capabilities available and on the position occupied in the city. For the environment to be cybersecure and cyber resilient, that is, to guarantee permanent urban service provision, the environment to be protected, the ecosystem and the participating actors must first all be identified. It must be understood that the risks associated with each service must be managed. Going forward, it is about planning activities, seeking collaboration between different parties, promoting ongoing formation and training, obtaining the necessary resources, and identifying the specific steps to follow. Cities must be proactive and show clear willingness to cooperate with all actors involved, to practice, to train, and to build capacities. It is surely worth the effort.

Sander Weeteling

Yiran Ding

References

AEPD (Agencia Española de Protección de Datos). 2017. "Código de buenas prácticas en protección de datos para proyectos *Big Data*." Madrid: AEPD. Available at https://www.aepd.es/es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf.

------. 2018. "Guía para Administraciones Locales." Madrid: AEPD. Available at https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf.

------. 2019a. "Guía Orientaciones y garantías en los procedimientos de anonimización de datos personales." Madrid: AEPD. Available at https://www.aepd.es/es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf.

------. 2019b. "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento." Madrid: AEPD. Available at https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf.

------. 2020a. "Adecuación al RGPD de tratamientos que incorporan inteligencia artificial: una introducción." Madrid: AEPD. Available at https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

------. 2020b. "Tecnologías y Protección de Datos en las AAPP." Madrid: AEPD. Available at https://www.aepd.es/es/media/guias/guia-tecnologias-admin-digital.pdf.

------. 2020c. Webinario AEPD "Smart Cities: Más allá de la seguridad, la privacidad de los ciudadanos." Madrid: AEPD. Available at https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/webinario-smart-cities.

------. 2021. "Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD." Madrid: AEPD. Available at https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

Agrafiotis, I. et al. 2018. Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity*, Vol. 4(1), tyy006. Available at https://doi.org/10.1093/cybsec/tyy006.

Alibasic, A., R. Al Junaibi, Z. Aung, W. Woon, and M. I. Omar. 2017. Cybersecurity for Smart Cities: A Brief Review. *Lecture Notes in Computer Science*, 10097: 22–30. Available at https://www.researchgate.net/publication/312528431_Cybersecurity_for_Smart_Cities_A_Brief_Review.

Article 29 Group. 2011. "Opinion 13/2011 On Geolocation Services On Smart Mobile Devices." Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

Barrero, V. 2018. "Estado de preparación en ciberseguridad del sector eléctrico en América Latina. Diagnóstico, recomendaciones y guía de buenas prácticas." Washington, D.C.: IDB, Comisión de Integración Energética de la Comunidad, Govertis. Available at https://publications.iadb.org/publications/spanish/document/Estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-America-Latina.pdf.

Biderman, C. et al. 2021. "Big Data for Sustainable Urban Development." Washington, D.C.: IDB. Available at https://publications.iadb.org/pt/big-data-para-o-desenvolvimento-urbano-sustentavel.

BlueVoyant. 2020. "State and Local Government Security Report." Available at https://www.bluevoyant.com/wp-content/uploads/2020/11/BlueVoyant-State-and-Local-Government-Report-26th-August-2020-FINAL.pdf.

Bouskela, M. et al. 2016. "The Road toward Smart Cities. Migrating from Traditional City Management to the Smart City." Washington, D.C.: IDB. Available at https://publications.iadb.org/es/la-ruta-hacia-las-smart-cities-migrando-de-una-gestion-tradicional-la-ciudad-inteligente.

CCN (Centro Criptológico Nacional). 2020. *Guía de Seguridad de las TIC*. CCN-STIC 803. ENS. Valoración de los sistemas. Madrid: Ministerio de Defensa. Available at https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html.

Cerdeira, P. et al. 2020. "Políticas públicas orientadas por datos: los caminos posibles para gobiernos locales." Washington, D.C.: IDB. Available at https://publications.iadb.org/publications/spanish/document/Politicas-publicas-orientadas-por-datos-los-caminos-posibles-para-gobiernos-locales.pdf.

Cerrudo, C., M. A. Asbini, and B. Russell. 2015. "Cyber Security Guidelines for Smart City Technology Adoption." Securing Smart Cities, pp. 1–17. Cloud Security Alliance (CSA). Available at https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf.

Crowdstrike. 2021. *Global Threat Report*. Available at https://www.crowdstrike.com/resources/reports/global-threat-report-es/.

CSIS (Center for Strategic & International Studies). 2021. "Significant Cyber Incidents since 2006." Washington, D.C.: CSIS. Available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/210804_Significant_Cyber_Events.pdf?bzKYK94rq5_3lrbYVK4fcL0rmkNq6lNI.

DHS/OCIA (Department of Homeland Security's Office of Cyber and Infrastructure Analysis). 2015. "The Future of Smart Cities: Cyber-Physical Infrastructure Risk." Washington, D.C.: DHA/OCIA. Available at https://us-cert.cisa.gov/ics/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk.

ECSO (European Cyber Security Organisation). 2018. "Smart Cities and Smart Buildings Sector Report. Cyber Security for the Smart Cities Sector, WG3 Sectoral Demand." Brussels: ECSO. Available at https://ecs-org.eu/documents/publications/5fdb27182b472.pdf.

Efthymiopoulos, M-P. 2016. Cyber-Security in Smart Cities: The Case of Dubai. *Journal of Innovation and Entrepreneurship*, 5(11). Available at https://doi.org/10.1186/s13731-016-0036-x.

Enerlis, Ernst, and Madrid Network Young. Ferrovial, 2012. "Libro Blanco Smart Cities." 1st edition. Available at http://www.innopro.es/pdfs/libro_blanco_smart_cities.pdf.

ENISA (European Union Agency for Network and Information Security). 2014. "Secure ICT Procurement in Electronic Communications. Analysis and Recommendations for Procuring ICT Securely in the Electronic Communications Sector." Heraclión: ENISA. Available at https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/at_download/fullReport.

------. 2015. "Cyber Security for Smart Cities: An Architecture Model for Public Transport." Heraclión: ENISA. Available at https://www.enisa.europa.eu/publications/smart-cities-architecture-model.

------. 2020. "Procurement Guidelines for Cybersecurity in Hospitals. Good Practices for the Security of Healthcare Services." Heraclión: ENISA. Available at https://www.enisa.europa.eu/publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/procurement-guidelines-full-version-es.pdf.

Eurocities. 2016. "EUROCITIES Statement on the Contractual Public–private Partnership on Cybersecurity." Brussels: Eurocities. Available at http://nws.eurocities.eu/MediaShell/media/EUROCITIES_cybersecurity_statement.pdf.

Forrest, C. 2019. Vendor Selection: What Needs to Be in a Good Policy. In: *ZDNet and TechRepublic, A Winning Strategy for Cybersecurity.* San Francisco, CA: CBS Interactive Inc. Available at http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

Gagliordi, N. 2019. Electronic Communications: What Needs to Be in a Good Policy. In: *ZDNet and TechRepublic, A Winning Strategy for Cybersecurity*. San Francisco, CA: CBS Interactive Inc. Available at http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

García, M., D. Forscey, and T. Blute. 2017. Beyond the Network: A Holistic Perspective on State Cybersecurity Governance. *Nebraska Law Review*. 96 (2). Available at https://digitalcommons.unl.edu/nlr/vol96/iss2/3/.

Global Smart Cities Alliance. G-20. 2020. "Model Policy. Cyber Accountability." Tokyo: World Economic Forum Centre for the Fourth Industrial Revolution, Japan. Available at http://globalsmartcitiesalliance.org/wp-content/uploads/2020/12/Cyber-accountability-v1.2-ESP.pdf.

Gómez de Ágreda, Á. 2020. Ciberseguridad en ciudades. In: *Las ciudades: agentes críticos para una transformación sostenible del mundo. Cuaderno de Estrategia 206*. Madrid: Instituto Español de Asuntos Estratégicos. Available at http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2020/Cuaderno_206.html.

ICO (Information Commissioner's Office). n.d. "Anonymisation: Managing Data Protection Risk Code of Practice." Wilmslow: ICO. Available at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

IDB (Inter-American Development Bank) and OAS (Organization of American States). 2020. "Cybersecurity Report 2020: Risks, Progress and the Way Forward in Latin America and the Caribbean." Washington, D.C.: IDB. Available at https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

INCIBE (Instituto Nacional de Ciberseguridad). 2016. "CEO, CISO, CIO... ¿Roles en ciberseguridad?" León, Spain: INCIBE. Available at https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad.

INCIBE-OSI (Oficina de Seguridad del Internauta). n.d. "Guía de ciberataques." León, Spain: INCIBE. Available at https://www.osi.es/es/guia-ciberataques.

Information System Authority. 2021. *Three-Level Baseline Security System ISKE*. Tallin: Republic of Estonia. Available at https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.

Interpol (International Criminal Police Organization). 2020. "Panorama mundial de la ciberamenaza relacionada con la COVID-19." Madrid, Spain: Interpol. Available at https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19.

IOActive. 2018. "Smart Cities Cyber Security Worries." Seattle, WA: IOActive. Available at https://ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf.

ISO (International Organization for Standardization). 2012. "ISO/IEC 27032:2012: Information Technology—Security Techniques—Guidelines for Cybersecurity." Geneva, Switzerland: ISO. Available at https://www.iso.org/standard/44375.html.

------. 2018. "SO/IEC 27005: Information Security Risk Management." Geneva: ISO. Available at https://www.iso.org/standard/75281.html.

ITU (International Telecommunication Union). 2008. "Clause 3.2.5 of Recommendation UIT-T X. 1205 (04/2008)." Geneva, Switzerland: ITU. Available at https://handle.itu.int/11.1002/1000/9136.

Kalinin, M. et al. 2021. Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines*, 9: 78. Available at https://doi.org/10.3390/machines9040078.

La French Tech. 2019. "C'est quoi La French Tech Rennes St Malo?" Rennes St Malo: La French Tech. Available at https://lafrenchtech-rennes.fr/.

Mantelero, A. 2017. "Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era." In: L. Taylor, L. Floridi, and B. van der Sloot (eds.), *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer. Available at https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf.

Martín, E. 2016. Smart Cities: El valor de construir ciudades inteligentes. *Revista TELOS*,105. Available at https://telos.fundaciontelefonica.com/archivo/numero105/el-valor-de-construir-ciudades-inteligentes-con-ciberseguridad/.

MIAC (Ministry of Internal Affairs and Communications). 2020. "Smart City Security Guidelines." Tokyo: MIAC. Available at https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf.

MINTIC (Ministerio de Tecnologías de la Información y las Comunicaciones). 2021. "Modelo de Seguridad y Privacidad de la Información, v. 4.0." Bogota: MINTIC. Available at https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

Muñoz, M. et al. 2018. "Guía de Buenas Prácticas sobre Smart City para pequeños y medianos municipios." Granada, Spain: Diputación de Granada, Red Granadina de Municipios hacia la Sostenibilidad (GRAMAS). Available at https://www.dipgra.es/uploaddoc/areas/349/SMARTCITY.pdf.

NCSC (National Counterintelligence and Security Center). 2021. "Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective." London, United Kingdom: NCSC. Available at https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf.

New America, N. Cohen, and B. Nussbaum. 2018. "Cybersecurity for the States: Lessons from Across America." Washington, D.C.: Cybersecurity Initiative, New America. Available at https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/.

------. 2019. "Smart Is Not Enough. How to Ensure the Technologies of the Future Don't Break Our Cities (and Us with Them)." Washington, D.C.: Cybersecurity Initiative, New America. Available at https://www.jstor.org/stable/resrep19969.1.

NIST (National Institute of Standards and Technology). 2008. "Guide for Mapping Types of Information and Information Systems to Security Categories. Special Publication 800-60 Volume I, Revision 1." Gaithersburg, MD: NIST. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152106.

------. 2019. "Smart and Secure Cities and Communities Challenge (SC3), GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook, Global City Teams Challenge 2019." Gaithersburg, MD: NIST. Available at https://www.nist.gov/publications/2019-global-city-teams-challenge-smart-and-secure-cities-and-communities-challenge-expo.

OAS (Organization of American States). 2019. "Data Classification. White paper series." Washington, D.C.: OAS. Available at https://www.oas.org/es/sms/cicte/docs/ESP-Clasificacion-de-Datos.pdf.

OECD (Organization for Economic Cooperation and Development). 2015. "Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document." Paris: OECD. Available at http://dx.doi.org/10.1787/9789264245471-en.

OSPI (Observatorio del Sector Público). 2017. "Ciberseguridad en el sector público. Documento de conclusiones." Available at https://www.ospi.es/export/sites/ospi/documents/informes/Informe_ciberseguridad.pdf.

Pandey, P. et al. 2020. "Making Smart Cities Cybersecure. Ways to Address Distinct Risks in an Increasingly Connected Urban Future." Deloitte Insights. Available at https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html.

PwC. 2021. "Global Digital Trust Insights Survey 2021. Cybersecurity Comes of Age." London: PwC. Available at https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights-2021.html.

Ranchordás S., and C. Goanta. 2020. The New City Regulators: Platform and Public Values in Smart and Sharing Cities. *Computer Law & Security Review*, 36. Available at https://doi.org/10.1016/j.clsr.2019.105375.

Razavi, A., S. Moschoyiannis, and P. Krause. 2009. An Open Digital Environment to Support Business Ecosystems. *Peer-To-Peer Networking and Applications*, 2(4): 367–97. Available at DOI:10.1007/s12083-009-0039-5.

Rea-Guaman, A. M., I. S. Sánchez-García, T. San Feliu Gilabert, and J. A. Calvo-Manzano Villalón. 2017. Modelos de madurez en ciberseguridad: una revisión sistemática. In: *12ª Conferencia Ibéricas de Sistemas y Tecnologías de la Información*, 21–24 June 2017, Lisbon, Portugal, pp. 284–89.

Salvador, C. 2021. Inteligencia artificial y gobernanza de datos en la administración pública: sentando las bases para su integración a nivel corporativo. In: R. Carles (coord.), *Repensando la Administración Pública. Administración digital e innovación pública*. Madrid, Spain: INAP. Available at https://www.libreriavirtuali.com/inicio/Administraci%C3%B3n-digital-e-innovaci%C3%B3n-p%C3%BAblica-Repensando-la-Administraci%C3%B3n-P%C3%BAblica-EBOOK-p306540049.

Shacklett, M. 2019. "10 Ways to Develop Cybersecurity Policies and Best Practices." In: *ZDNet and TechRepublic, A Winning Strategy for Cybersecurity*. San Francisco, CA: CBS Interactive Inc. Available at http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

Soare, S., and J. Burton. 2020. "Smart Cities, Cyber Warfare and Social Disorder. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence." Available at https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.pdf.

Stilgherrian. 2019. "Security Training Is Useless Unless It Changes Behaviours." In: *ZDNet and TechRepublic, A Winning Strategy for Cybersecurity*. San Francisco, CA: CBS Interactive Inc. Available at http://book.itep.ru/depository/security/surveys/SF_feb2019_cybersec.pdf.

Townsend, A., and P. Zambrano-Barragán. 2019. "Big Urban Data. A Strategic Guide for Cities." Washington, D.C.: IDB. Available at https://publications.iadb.org/publications/spanish/document/BIG_Data_urbana_Una_gu%C3%ADa_estrat%C3%A9gica_para_ciudades.pdf.

Trapenberg, F. et al. 2021. "The Cybersecurity Risks of Smart City Technologies, What Do the Experts Think?" UC Berkeley, CLTC White Paper Series. Available at https://cltc.berkeley.edu/2021/03/16/smart-cities/.

UNE (Asociación Española de Normalización). 2021. "Comité CNT 178: Ciudades inteligentes." Madrid: UNE. Available at https://www.une.org/encuentra-tu-norma/comites-tecnicos-de-normalizacion/comite?c=CTN%20178.

WEF (World Economic Forum). 2021. Whitepaper, Governing Smart Cities: Policy Benchmarks for Ethical and Responsible Smart City Development. Geneva: WEF and Deloitte. Available at https://www.weforum.org/whitepapers/governing-smart-cities-policy-benchmarks-for-ethical-and-responsible-smart-city-development.

A Cybersecurity Guide for Smart Cities

AUTHORS: Lorenzo **Cotino**
Marco **Sánchez**

EDITORS: Mauricio **Bouskela**
Gilberto **Chona**
Ariel **Nowersztern**
Patricio **Zambrano-Barragán**
Isabelle **Zapparoli**

IDB