In collaboration with
Deloitte

WORLD ECONOMIC FORUM

# Accountability for Cybersecurity

## BENCHMARK REPORT

JULY 2021

This publication forms part of a suite of benchmark reports produced by the G20 Global Smart Cities Alliance to analyse trends in smart city governance across the 36 Pioneer Cities of the Alliance.

## Introduction

As municipal authorities and services become more connected through procurement of smart city solutions, exposure to cybersecurity risks increases. Cybersecurity should be a high priority for any city, even in the absence of a smart city agenda, as cybersecurity threats exist everywhere. Designating responsibility and accountability for cybersecurity is a step towards protecting a city and its public services against cyberthreats. According to the model policy, one senior officer or a group of key senior individuals within a city should have the ultimate responsibility for cybersecurity and any breaches of security. This person or group should evaluate, direct and monitor the design and deployment of effective information security measures for smart services, and be answerable for the response to and recovery from any cyber incident. There should also be full buy-in from the executive city leadership.

Some 28 Pioneer Cities provided details of their cyber accountability policies. Figure 1 shows the extent to which a policy for cybersecurity accountability has been adopted in these Pioneer Cities.

## Key findings

- Accountability to senior leaders is a key requirement in the model policy. A senior official should be given the responsibility for cybersecurity and a cybersecurity plan should be reviewed regularly by senior management. **Less than half of Pioneer Cities have met these basic requirements for senior accountability** (13/28 cities) (Figure 1).
- Cities should have a governance framework that is reviewed regularly. **Senior management carry out regular reviews of the cybersecurity governance framework or plan in about half of the Pioneer Cities** (15/28 cities).[1]

> **Dubai has set up an office for cybersecurity in each of 133 government entities and semi-entities. The cybersecurity governance framework is reviewed annually by the director-general's office, which functions as an audit practice."**[2]
>
> **Dubai**, UAE

- To understand the potential cybersecurity risks, a senior responsible officer needs to have an up-to-date inventory of the city's information and communications technology (ICT) infrastructure and assets, including devices, users, networks, data and applications. This also should include operational technology as well as information technology assets. **More than half of Pioneer Cities, and most in Europe, maintain an up-to-date inventory** (18/28 cities).[3] Most Pioneer Cities in Europe state that their data inventories are up to date. This could be due largely to the implementation of General Data Protection Regulation (GDPR) regulations in the European Union.[4]
- The officer responsible for an up-to-date inventory needs to be informed about new technology deployments that will add to this inventory. This is to ensure that minimum standards are adhered to for new ICT deployments. **In less than half of Pioneer Cities, the IT function is not always informed about new technology deployments** (11/28 cities).[5] This means that the IT function may be out of the loop and unaware of new technology assets in less than half of these cities.

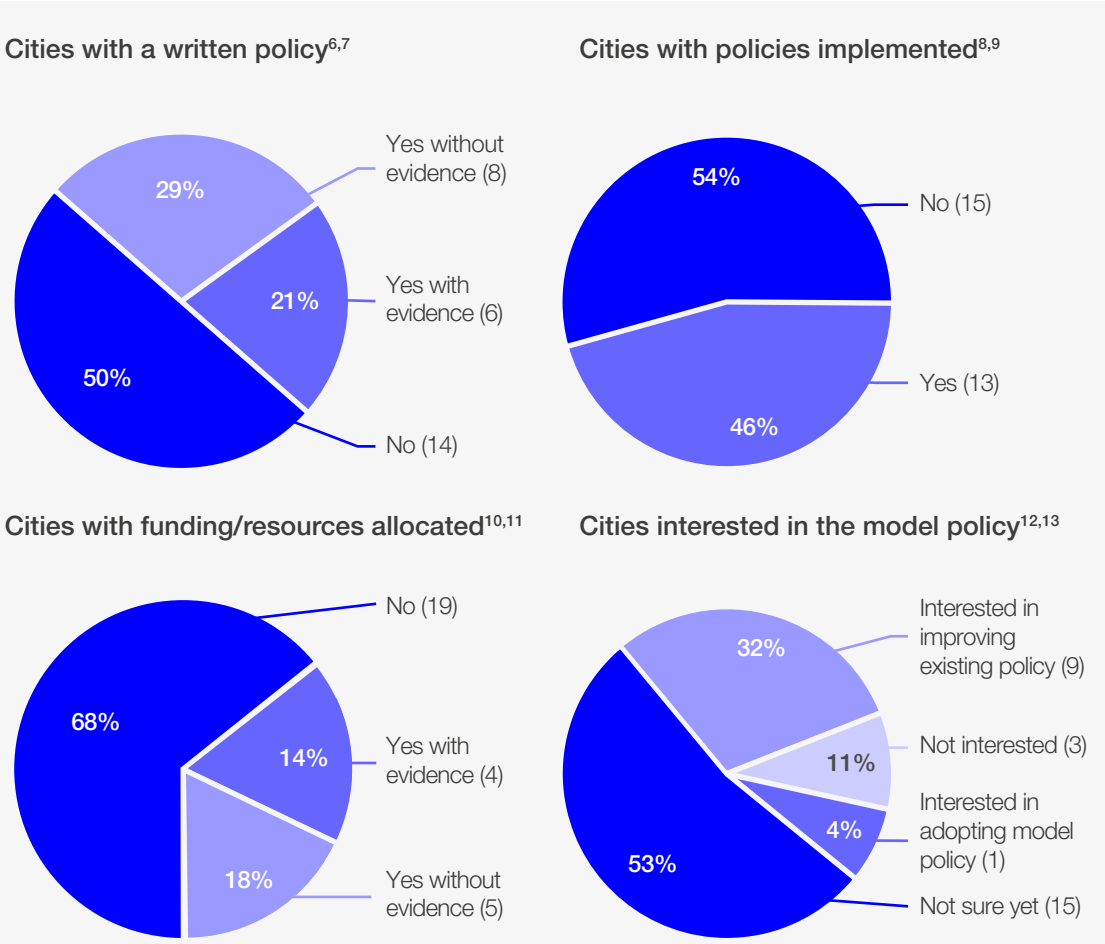
## The current state of play

Compared to other model policies in our assessment, the Pioneer Cities have made good progress with this model policy. This may reflect the seriousness of the cyberthreats cities face. Even so, cities should consider areas for improvement, particularly if they do not yet apply the model policy recommendations:

- Establish a structure for senior leaders to be informed about cybersecurity in their smart city deployments and other systems and be accountable for them
- Develop a better way to understand cybersecurity risks to which the city is exposed across all departments

More guidance on these points can be found in the model policy.

FIGURE 1 **Adoption and implementation of policies for cybersecurity accountability**




**Source:** Deloitte analysis of Pioneer City Policy Assessment data, March 2021

## Contributors

### World Economic Forum

**Yuta Hirayama**, Project Lead, Internet of Things and Urban Transformation

**Jeff Merritt**, Head, Internet of Things and Urban Transformation

**Rushi Rama**, Smart Cities Lead, Internet of Things and Urban Transformation

### Deloitte

**Miguel Eiras Antunes**, Global Smart Cities Leader, Deloitte Global, Portugal

**Mahesh Kelkar**, Executive Manager, Center for Government Insights, Deloitte, India

**Shuichi Kuroishi**, Manager, Deloitte, Japan; Secondee to the World Economic Forum

**Miwa Ono**, Manager, Deloitte, Japan

**Oki Sakuyama**, Consultant, Deloitte, Japan

**Yoshitaka Tanaka**, Consulting Chief Strategy Officer, Deloitte, Japan



## Acknowledgements

### G20 Global Smart Cities Alliance Policy Task Force

### Lead:

**Yalena Coleman**, Applied Data and Technology, Connected Places Catapult

### Members:

**Abhik Chaudhuri**, Chevening Fellow, Tata Consultancy Services

**Daniel Dobrygowski**, Head of Governance and Trust, World Economic Forum

**Saj Huq**, Director, London Office for Rapid Cybersecurity Advancement

**Eleri Jones**, Head of PETRAS National Centre of Excellence for IoT Cybersecurity, University College London

**Tadashi Kaji**, Distinguished Researcher, Hitachi

**Michael Lake**, Chief Executive Officer, Leading Cities

**Xiaodong Lee**, Founder and Chief Executive Officer, Fuxi Institution

**Greg McCarthy**, Chief Information Security Officer, City of Boston

**Murray Rosenthal**, Senior Policy Analyst (Security), City of Toronto

**Mirel Sehic**, Cybersecurity Director, Honeywell

**Sandy Tung**, Programme Manager, Greater London Authority

### Contributing Pioneer Cities

- Apeldoorn, Netherlands
- Belfast, United Kingdom
- Bilbao, Spain
- Bogota, Colombia
- Brasilia, Brazil
- Chattanooga, United States
- Cordoba, Argentina
- Daegu, South Korea
- Dubai, United Arab Emirates
- eThekwini, South Africa
- Faridabad, India
- Gaziantep, Turkey
- Hamamatsu, Japan
- Hyderabad, India
- Indore, India
- Istanbul, Turkey
- Kaga, Japan
- Kakogawa, Japan
- Kampala, Uganda
- Karlsruhe, Germany
- Leeds, United Kingdom
- Lisbon, Portugal
- London, United Kingdom
- Maebashi, Japan
- Manila, Philippines
- Mexico City, Mexico
- Milan, Italy
- Newcastle, Australia

## Endnotes

1. CA5.1: “Does your city’s senior leadership review a cybersecurity governance framework or plan on a regular basis (e.g. once per year)?”
2. Interview with city officials of Dubai, conducted on 18/3/21, on Zoom.
3. CA5.2 “Does your city have an up-to-date inventory of existing infrastructure including devices, users, networks, data and applications which might affect the city’s cyber threat landscape?”
4. Intersoft Consulting, “General Data Protection Regulation GDPR”, May 2018: https://gdpr-info.eu(link as of 14/6/21).
5. CA5.4: “Do city departments always inform IT or your senior responsible officer before any new procurements of technology solutions?”
6. Pioneer City Assessment Survey CA2.1: “Does your city have a written policy (or set of policies) that defines which senior officer(s) in the city has accountability for cybersecurity?”
7. CA2.3: “Please share a link to the most relevant document – link.”
8. CA3.1: “Please provide the job title of the senior officer with direct accountability for the following cyber-related duties.”
9. CA5.1: “Does your city’s senior leadership review a cybersecurity governance framework or plan on a regular basis (e.g. once per year)?”
10. CA4.2: “Are there resources or funding available in your city government to ensure privacy impact is assessed for new technologies?”
11. CA4.3: “Please describe these resources – funding/budget per year.”
12. CA7.4: “Having reviewed the model policy, will your city work towards adopting the model policy or some version of it in the future?”
13. CPPF2.1: “Please select all model policies that your city will be working on in future stages of the Pioneer Programme (including attending workshops and developing policy proposals).”

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org