# Cybersecurity in governments and smart cities

With 18+ years' of public sector experience Massimiliano Claps, Research Director, IDC European Government Insights, shares his expertise and provides insight about the security issues confronting governments and cities today.

Brochure

Alcatel·Lucent Enterprise

# The state of cybersecurity in governments and smart cities today

Over the last 25 years, since IDC has been tracking the use of technology in the public sector at both the central government level and city level, there's been an important evolution. As little as 20 years ago, the strategic direction was to get services and information online. This included very basic offerings such as downloadable forms. It's been a long journey to where we are now with public sector offerings that include interactive services on multiple channels, and mobile apps, and using social media to increase public awareness about available services and programs.

At the city level, when we started researching the public sector, terms like smart cities didn't even exist and local and regional government were busy with the legacy systems that they had, dealing with building permits, business licensing and code enforcement. And then cities evolved to where digital became more pervasive and technology is now used in operational processes and integral to transportation, infrastructure maintenance, and environmental monitoring. **The expanded role of digital at both the central government and city levels has blurred the line of protecting these digital assets.**

## The changing face of public sector threats

In the early days, if you were setting up a website with citizen information, public sector entities could be open to the internet through some gateway that would have to be protected from viruses, trojans and phishing attacks. Today, operational technology is subject to Distributed Denial of Service (DDOS) attacks and ransomware.

**While the number of threats is not necessarily going down, the type of threats and sources are becoming more differentiated and continuously changing, which is making cybersecurity a very high priority for government officials.**

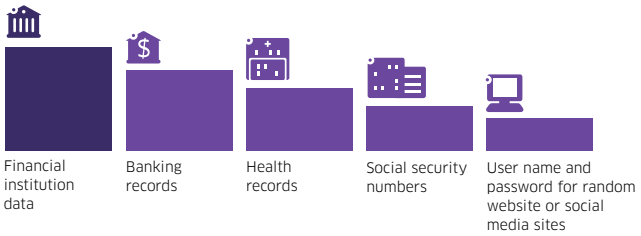
At the end of 2019 IDC interviewed approximately 290 government IT executive across several European countries.

**60%**

of the central government executives said improving detection and resilience against initial attacks was a business priority for their government organisation, not just an IT priority.

**56%**

of the local and regional government officials said the same.




## Hacker targets in the public sector

While there is some debate, generally speaking there are certain types of data that hackers consider more valuable than others. For example:

- Financial institution data
- Banking records
- Health records
- Social security numbers
- and then towards the bottom you find user name and password for random website or social media sites

Governments typically collect data related to healthcare and social security, making them a target. Also, government data, such as a taxpayer ID or a social security number is valid for life, while banking credentials, once stolen, can be deleted from the system and replaced with new ones.[1] Other industries such as financial organisations are equally interesting to hackers.

## Skills and budgets impact data privacy and regulatory compliance

Some of the key cybersecurity challenges for business and IT executives in government include data privacy and compliance with new regulation such as the NIS directive, shortage of skills and difficulty in making the case for cybersecurity investments. The challenges are highly interdependent because the shortage of skills, and budgets make it difficult to comply with all new regulations, creating exposure to further risks. The impact of these challenges is not the same across central and local governments. For example, in our study 30% of central governments responded that managing regulatory compliance is a business priority, however, 51% of local and regional governments see it as an important element.

**This doesn't mean that central governments don't care about regulatory compliance, it means that they have larger departments and with the skilled personnel to deal with vulnerabilities, and implement solutions for governance and compliance, whereas small-to-medium-sized municipalities struggle to comply with new regulations and to implement best practices.**

**30%**

of central governments responded that managing regulatory compliance is a business priority

**51%**

of the local and regional governments see it as an important element

1. https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/

## Smart city data: A different type of target for hackers

Smart cities create a different dynamic for hackers. It's a matter of scale of complexity that increases, because it's not just a cybersecurity problem, but operational security problems and physical security problems. For example, smart cities deal with video surveillance, access points, and securing legacy systems, such as energy grids, water pumps, and traffic signaling.

**It's not a matter of city data being more valuable than central government data. It's that the threat landscape is different. All of these other points of exposure to operational technology and physical security make it more complex to assess and monitor vulnerabilities.** They are subject to more DDOS attacks and ransomware as well, but in a different context compared to a large tax or welfare agency at the national level.

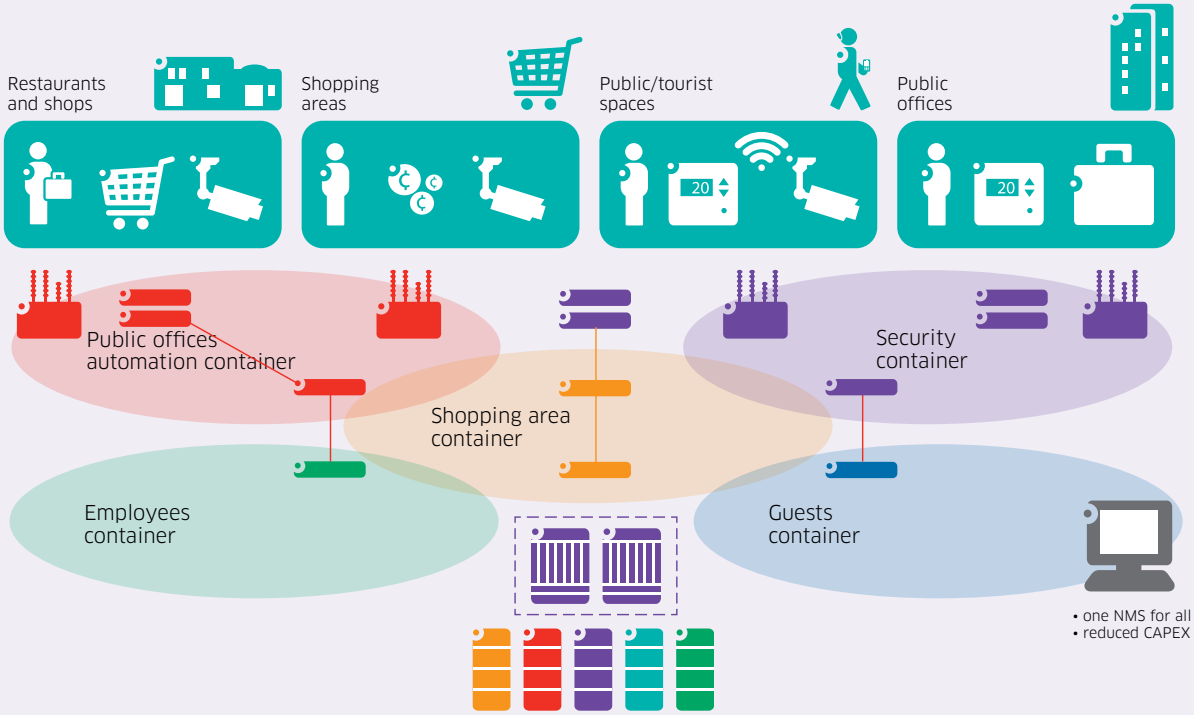


### SOLUTION HIGHLIGHT

**Reduced vulnerability with containerization and segmentation**

The Alcatel-Lucent IoT Digital Business solution allows smart cities and public sector organizations to containerize each device, creating a virtual network segment for it to prevent any device from becoming a vector for attacks. Containerization makes multiple virtual networks out of a single physical network, which is managed by a single management system.

**Figure 1: Multiple virtual private networks over one physical IoT network**



# Cybersecurity readiness

According to a number of studies on the state of security automation by industry – the public sector is among the least prepared in the area of security automation.

Organisations in the public sector took the most time to identify and contain a cyberattack after healthcare organisations, 231 days and 324 days, respectively. And the longer it takes to identify and contain, the higher the costs.

**Figure 2: Days to identify and contain a data breach by industry sector[2]**

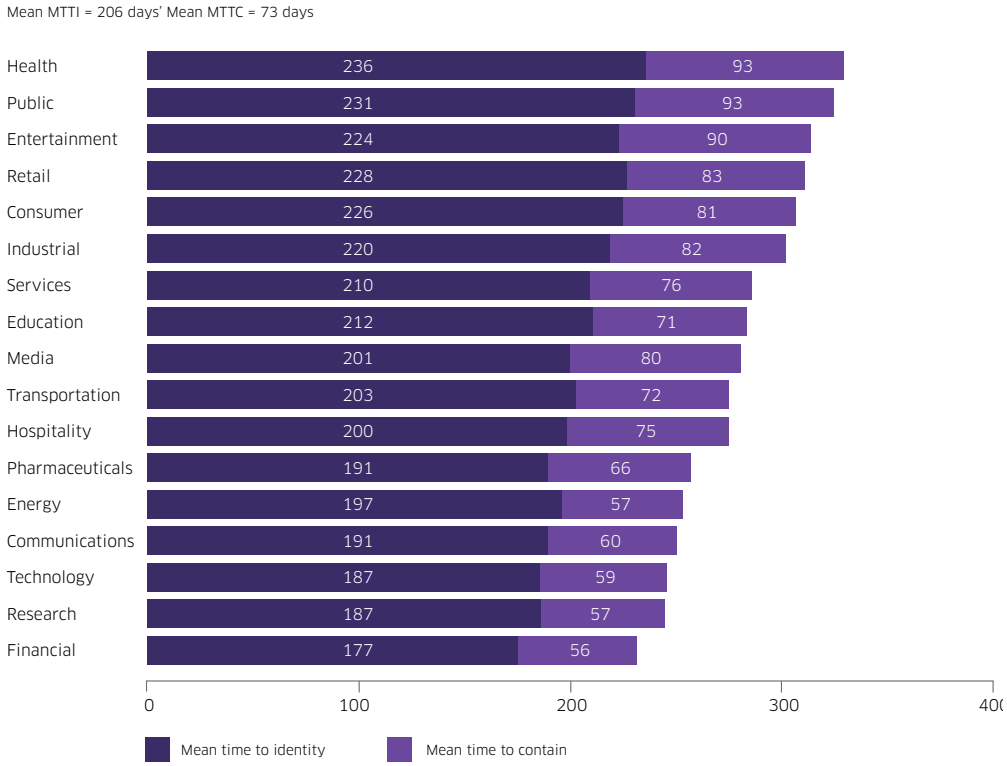
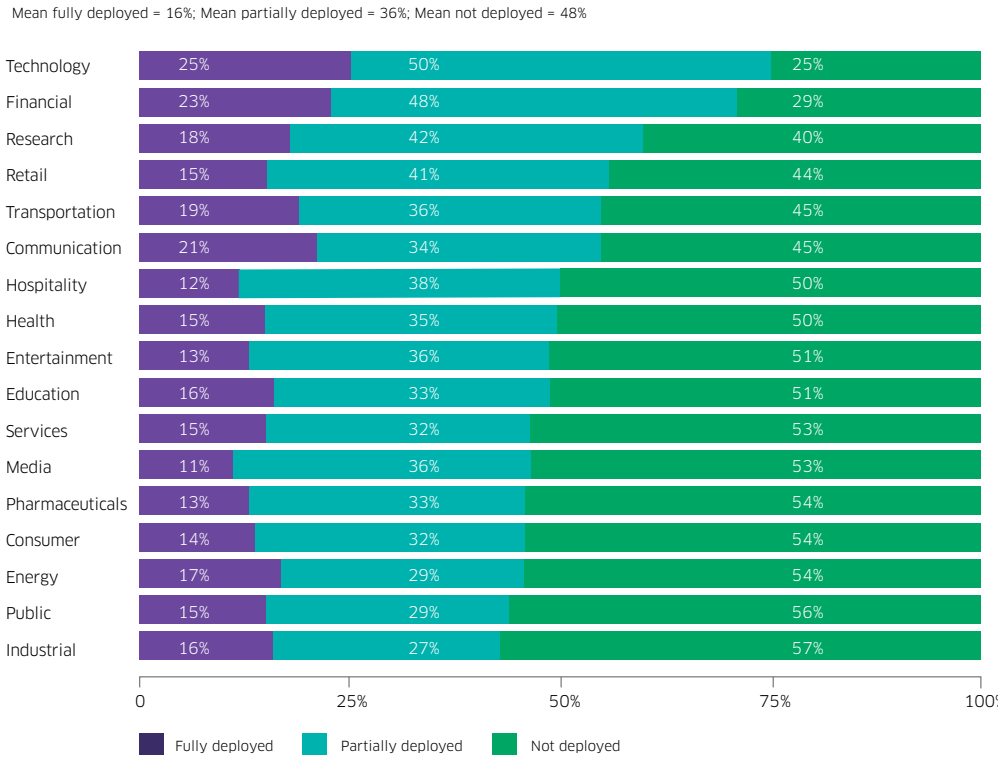



**Figure 3: State of deployment[2] (These statistics apply in general to the public section everywhere beyond Asia.)**




2. IBM Security: Cost of a Data Breach Report
https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.214883607.1034594978.1579101338-1286175879.1579101338

## Cybersecurity readiness factors

There are a number of different levels of maturity and readiness factors that can impact an industry's ability to adopt security policies. Following are three elements to consider: skills, processes and budgets.

- **Skills**

  Much of the public sector workforce began working with IT and dealing with IT assets a very long time ago. If you look at the average age of government employees in some European countries there's clearly a set of skills that entered the workforce many years ago. Since then there have been many technology advancements. Skills that were nurtured in the early days of client servers and the Internet are not the same skills required today for Artificial Intelligence (AI), Internet of Things (IoT) and Blockchain, among others.

- **Processes**

  **A lot of cybersecurity processes and operations are asset centric.** Securing a laptop or server, a data center or a LAN, is different than securing users that are dependent on roles and credentials. Different approaches in terms of cybersecurity are required and the workforce may not have the skills to deal with these new demands. Technology innovation, particularly in terms of AI and automation is changing the way security functions are performed, which only amplifies the skills gap.

- **Budgets**

  Justifying investment in cybersecurity is not without its challenges, particularly during a global health crisis when governments are shifting budgets to support public health resilience and economic recovery. Measuring the benefits of additional cybersecurity investment is difficult and accounting for additional resources can be complicated.

### Public sector employees are aging

- *The average age of an Italian public sector employee in 2001 was 43 years old.* ***Now the average age is over 50 years old****.*
- ***The current average age of US public sector employees is 45.4****, according to the Bureau of Labor Statistics (BLS) in 2019.*
- ***More civil servants are in the 50–59 (32%) year old age band*** *than in any other according to the UK Institute of Government*
- ***Almost one in two French public service agents are 50 or older*** *(Le Portail de la Fonction Publique)*
- *The median age of the labour force is projected to increase everywhere, but* ***the pace of increase is fastest in Asia and the Pacific*** *(The International Labour Organisation)*

## Addressing security challenges more efficiently

It all starts with making security relevant at every stage of the systems' lifecycle. The governance model that helps align IT supply and demand in the public sector used to be quite traditional. A group of people focussed on developing an application, and then they handed over something to the infrastructure and operations teams, who would then make it work in the data center and apply security as one of the wave-two activities after everything was ready from application stand point.

Third-wave platform technologies, which included cloud, big data and analytics, mobile computing and social computing, disrupted the traditional IT governance and operating models. Internal IT governance and the advent of practices such as DevOps made it very clear that interdependencies existed. Developing an application, such as BI or ERP, a citizen service, a website, or a public sector application, was very much related to how that app would run in the cloud – public, hybrid, or private – and whether it would be exposed in an app or consumed through a smartphone. If security was not added early on in the app development and testing stages, challenges would arise because of the many devices, channels, and networks that the delivery of the service would rely upon. In such a scenario, securing the device, or a piece of the network, or encrypting a connection would not be sufficient.

The public sector is slowly catching up and doing quite a bit a work, around DevOps or DevSecOps, and thinking about the entire lifecycle of systems and the fact that security is relevant at every stage from the early inception and design, all the way to sunsetting the application. They must make sure that no one has credentials to use the app when it's been cleared out of the asset inventory for a certain public sector entity. They must ensure there are no data in someone's memory stick, or a client version on someone's laptop that is no longer authorized for use.

Security at every stage is an important element that still needs to be embedded in cybersecurity strategy and processes. Governments are getting there, they are much more aware than they were four or five years ago.




Costs that are reported in the newspapers and media are not necessarily the ones that most impact day-to-day activity. The fact that a local council paid a ransom may not, in fact, be the largest impact.

## Impact and cost of cybersecurity incidents

Identifying the cost of security can be difficult. There are many elements to consider such as:

- Direct costs: Triage costs associated with an attack
- Forensic costs
- Recovery costs
- Financial losses
- Productivity loss
- Operational technology disruption from DDoS
- Ransom payments
- Legal fees

There is a long list of direct and indirect costs, as well as both short and long-term impacts, reflected in accounting systems, that are hard to quantify. Costs that are reported in the newspapers and media are not necessarily the ones that most impact day-to-day activity. The fact that a local council paid a ransom may not, in fact, be the largest impact. A fine that may be incurred due to non-compliance with the General Data Protection Regulation (GDPR); the need to acquire digital forensic tools to investigate the breach; net new investment triggered by the breach to implement a threat monitoring dashboard, are all costs associated with cyber attacks that must be accounted.

**It's not just the immediate direct cost that governments and cities need to consider. There is a spectrum of impact on operations and productivity as well as a loss of trust that citizens experience with regard to the acceptable use of technology by governments. A holistic view is required when assessing the cost of a breach.**

The average organisational cost globally is $3.92 million USD and the average number per records per breach is 25,575, which cause concern among CIOs and CISOs, as the Allianz Risk Barometer demonstrates.

# Decreasing the cost of a breach: IDC recommendations

There are three things governments need to consider to decrease the costs associated with a breach. These include:

1. A holistic view of costs and value of cybersecurity which can help in justifying the budget
2. Consider different ways of providing cybersecurity from the perspective of services and users rather than assets
3. Nurturing cybersecurity skills for governments who want to tackle the risks associated with cyber attacks

**A holistic view of security** allows organisations to better prioritize costs. For example, if a ransomware is only 10% of the overall cost, they may decide to not pay it, but instead invest in tools that prevent cyber attacks such as DDoS that put people at risk, for example on a transportation systems where the traffic lights are not working. Accounting for value and cost of security in a more thorough manner is essential.

**Consider cybersecurity from the perspective of services:** If you look at security in terms of identity management, vulnerability, and trust management, a strategy and security model that looks at the services provided, and less at the assets, is also very important. The world has changed. The context of technology has changed. The way in which security services are delivered has changed. Think about services and users. They need business applications delivered securely, regardless of where they are or what devices they're using.

**Nurturing skills,** providing training, and increasing IT literacy for all the users, not just cybersecurity experts is important. Breaches happen when personnel are not aware of the risks associated with cybersecurity incidents such as inadvertently misplacing data. Nurturing cybersecurity skills in general, not just deep dive technical skills, and AI, is important.

# Top cybersecurity threats

Ransomware has gotten a lot of attention, probably because local governments and healthcare institutions are a primary target of this type of attacks. However, interestingly during the recent global health crisis some of these attacks have decreased.

### IoT attacks

The complexity of IoT-based attacks is changing which is something cities will have to pay increasing attention to.

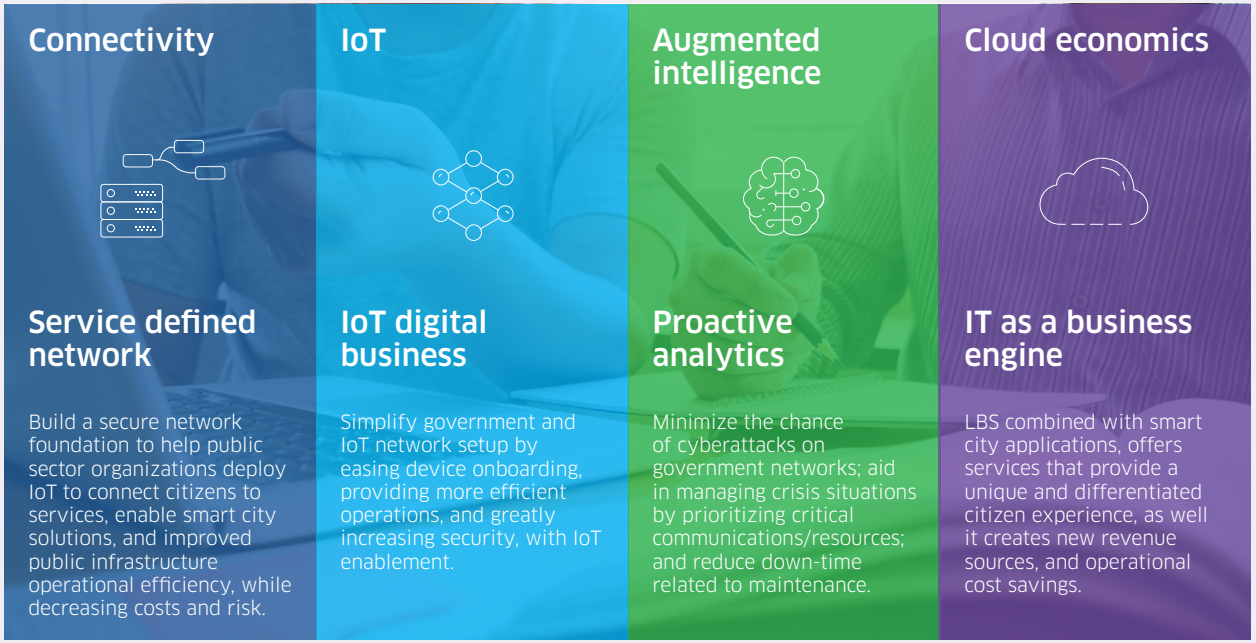
- **Multiple connection points and parties:** From a business perspective, utilities, management collection, and transportation are often contracted out to other companies. This means that from a process orchestration point of view there are things that a municipal government cannot control, and a wider perimeter that exposes them to risk.
- **The complexity of the networks and management:** Networks that support IoT and edge devices are becoming more complicated: Some data may reside on the edge with edge devices running an app connected to the cloud to trigger alerts when anomalies are detected. A limited set of data is sent to the core on-premises data center. There are many complexities to be managed: from f spoofing the edge device, to encrypting the transmission from the edge device to the core data center, to protecting the connection for the app process that is pushed from the cloud to the edge.

**SOLUTION HIGHLIGHT**

**Digital Age Networking**

Alcatel-Lucent Digital Age Networking in Government is a multi-faceted approach to government network cybersecurity that provides security in depth for connected smart city devices and applications through multiple layers of security.

- **Digital Age Networking provides**: A Service Defined Network enabling connectivity that spans from the datacenter, to the access layer. It allows you to easily, automatically, and securely connect people, processes, applications, and objects, which enables digital transformation.



At the end of 2019 IDC asked clients about their IT security priorities for 2020.

**42%**

of local and regional government said that mobile device security is important

**38%**

Operational technology security was mentioned by local and regional government

**34%**

of local and regional government identified edge point security

**32%**

in central government felt the same

**19%**

and only central government executives

**26%**

of central government mentioned it

## Cybersecurity threats: Connected and mobile devices

According to a recent survey conducted by IDC, data indicates that IoT and operational technology are a concern for local and regional government.

The mobile devices used by police officers, building inspectors, social care workers on a daily basis, as well as the IoT devices embedded in traffic counting and signaling systems, video surveillance cameras, energy management systems in the city ecosystem are very relevant and of increasing concern.

Securing all IoT connectivity is impossible as it becomes more and more pervasive. And, it can definitely impact citizen safety, because if traffic lights don't work accidents happen; if water systems don't work there can be flooding; not to mention in healthcare, if a procedure using robotic equipment is subject to an attack, there are clear risks to individual safety.

**How to deal with security for connected devices**

- **Apply cybersecurity tools and practices to technologies that were not originally engineered to accommodate them.** When the first traffic signaling systems were built they were not designed to be connected to an IP network, and now increasingly, they are, so there need to be some technical work to embed solutions to protect the operational assets that were not designed with security in mind.
- **Identify where the assets are located.** Cities have an increasing inventory of digital assets across different departments. For example, the police may know how many cameras are out there; the transportation department may know the number and location of traffic lights; and someone from utilities may know about the public lighting system. Managing the inventory and assessing the vulnerability of these assets is a complex task in itself and it needs to be carried out before solutions can be applied to protect the assets.
- **Continuously monitor the assets** because even once the solutions are in place, new forms of attacks will need to be detected and remediated quickly, and more modern solutions will need to be applied.

**SOLUTION HIGHLIGHT**

**Ensure city assets security with asset tracking**

Alcatel-Lucent OmniAccess® Stellar Asset Tracking provides smart connection to assets, so you can locate equipment and people in real-time, optimizing operations and reducing costs.

The complexity will continue to increase as attacks types change and require a more thorough approach in terms of understanding the architecture in place; continuously monitoring using services such as remote monitoring services, virtual security operation centers, among others, and then continuously improving those cyber security services in cities.

**Based on IDC surveys we see IT and IoT security is as top of mind concern for cities and local and central governments.**

The geo-politics in terms of who is the provider of equipment also needs to be considered. With the evolution to 5G, we are encountering a debate around certain network equipment suppliers being used in certain countries or not, or in only certain parts of the network architecture, and not core sensitive services.

### Analysing mobile and IoT devices vulnerability

There are practices out there for assessing the vulnerability of mobile and IoT devices, such as the vulnerability scoring systems that can help IT executives in government organisations prioritize resources and determine where they need to apply security procedures for certain groups of users and devices.

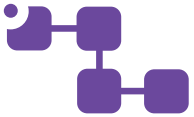
**The vulnerability analysis needs to get more granular when it comes to understanding the vulnerability and the number of devices, use cases that the devices support, and the number of networks they connect to** (for example; Wi-Fi, device-to-device Bluetooth connection, LTE set-up for a public security force as proprietary network, or public 4G/5G network). All of these continuous changes of profiles, impact the vulnerability aspect of a device and make it complex to deal with a network perimeter that is no longer under direct control of the public sector entity. Geofencing can complement other cybersecurity tools and practices already in place to help protect public institutions.

## Recommendations for government organisations to increase their cybersecurity posture

Following are key components to improve security in government and smart cities.

- **Skills, is definitely an important one.** Skills both for the experts that need to move from being experts in anti-virus software or firewalls into being more expert on risk assessment and management capabilities, threat monitoring, response, digital forensics, so the type of skills changes
- **The cybersecurity processes** need to change from an asset-centric to an end-to-end user-centric service that needs to be delivered
- **The ability to quantify and justify the value and cost of cybersecurity to secure budget.** Eventually, the head of government agency or the mayor will have to answer the question: "Have we allocated sufficient resources to protect critical assets versus have we spent enough money to afford public transportation?" To answer the question from a cybersecurity perspective, the CIO or the IT Security manager will have to evaluate the three dimensions of cost, risk, and value, and optimize the allocation of resources based on risk reduced per unit of cost and other indicators. As mentioned previously, the cost management and justification factor, and the ability to allocate sufficient budget for cybersecurity is the third element after skills and processes.

Cybersecurity skills



Cybersecurity processes

Ability to quantify and secure cybersecurity budget

# Improve network infrastructure cybersecurity

Governments that want to implement an end-to-end service-centric approach to security, need to protect all layers of the service, from the network to the software.

Starting at the top, at the software layer, the whole application life-cycle needs to be taken into account. Testing tools can assess the vulnerability of an application when developing the code, providing information about how it leverages APIs from systems, or how it processes a certain form that exposes it to an attack, or exposes the data when it's running across a hybrid cloud infrastructure.

The application piece requires greater and greater attention – dynamic and static application testing tools that can identify if there are security risks in how the code is written and how it will run in a certain operating environment is an important one that is not always given the attention that it should have.

## Geofencing enhances protection for public institutions

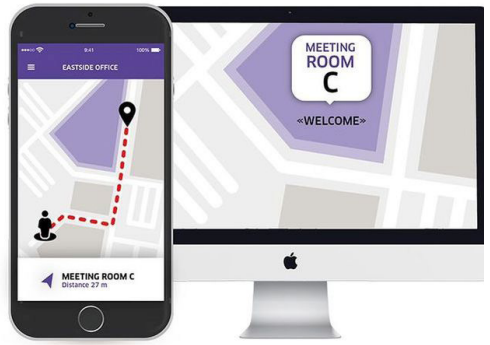
Geofencing can complement other cybersecurity tools and practices already in place to help protect public institutions.

Geofencing is the concept of changing the levels of protection or authorization of a specific user to enable certain actions, or focus on monitoring threats in a dynamic manner depending where that person is. For example, it's one thing if you're using your laptop in the office and you're attached to the local area network, however, it's a totally different thing if you're using your own laptop (BYOD) and trying to connect remotely to your system with or without a VPN – this creates exposure to different kind of threats. Being able to dynamically change the way security is applied, based on position – creating higher or lower risk locations – is helpful. GPS versus Wi-Fi and Bluetooth location data has a different impact in terms of battery consumption for devices but also for example, in terms of offering protection of the access keys.

**SOLUTION HIGHLIGHT**

Alcatel-Lucent OmniAccess Stellar Location-based Service (LBS) such as indoor wayfinding navigation, asset and people tracking enable government organizations to set up policies that take user or asset location into account.


OmniAccess Stellar Location Based Services
Indoor positioning




OmniAccess Stellar Location Based Services Geofencing

## A cloud solution with built-in security can reduce vulnerabilities

Cloud solutions with built-in security help reduce vulnerabilities, because cloud providers are typically large operators with the critical mass to invest in modern, up-to-date cybersecurity skills, tools, processes and practices.

Worrying about data residing on edge devices or servers sitting in a cabinet that manages traffic lights or video cameras versus a smartphone is much more complicated. Centralization enabled by the cloud in a distributed computing environment helps with security, but also creates other issues that IT managers need to consider. **From a pure security aspect the cloud can be more secure; however, you also need to consider efficiency, data compliance and safeguarding.**

- **Efficiency**

  Do you really want to send to the cloud, every frame captured by video cameras when there are thousands of video cameras? You must make a choice and apply a data policy for efficiency. For example, only send anomalies to the cloud and delete all the other data 24 hours after it is captured by the edge device. In this scenario, the data never leaves the edge device.

- **Data loss, compliance and safeguarding data**

  While the cloud is more secure, if something does happen you're dependent on a mega cloud computing data center and if there's no back-up data anywhere else, that data could be lost. There are a number of public entities, who even though they are eagerly migrating to public cloud services, are setting up their contract and architecture so that they have a back-up of sensitive data in a different data center, and are not reliant on one data center.

**SOLUTION HIGHLIGHT**

**Discover Alcatel-Lucent Rainbow™**, the secure cloud collaboration service for public services, administration and schools. With Rainbow you get a secure collaboration alternative, compliant with GDPR, ISO 27001 (HDS – health data security for France) and ISO 27017/18 (privacy in the cloud) - with end-to-end SSL encryption. All without the need of a mobile phone number, and for any mobile device. You can use WebRTC telephony and video or hold conferences.

Rainbow™

# Cybersecurity strategies to deliver secure digital services

Clearly the recent global health crisis has changed the way the world operates. It **accelerated the need to deliver services digitally**, for example, the courts in the UK started holding online hearings, other services went virtual and civil servants started working from home. These actions have resulted in reduced physical control of the managed devices and where they were accessed from in the network.

**Remotely enforcing cybersecurity policies defined by the government has helped, however, consistency is a problem as controlling every single access point and device is not possible.**

Before working from home was so extensive, it was easier to standardize the devices, network and components. Now there are multiple exceptions in terms of device, identity, type of authentication, infrastructure policies, dependency from operator, and visibility.

**Visibility is a big issue.** Even though remote monitoring helps, security teams are no longer working hands-on, there's a lot of channel IT, and incidents that are only reported days later to the IT security team, making it difficult for them to ensure continuous support as routines get disrupted. In addition maintaining the right inventory of assets to respond to incidents can be challenging.

The level of control and visibility as well as the continuity of security processes was disrupted. Governments had to take into account the fact there was an extended network to worry about.

**Addressing the visibility challenge: Elements to consider**

- First line of defense was to **set up a number of VPN connections**
- **Identity and access management must be more dynamic**, as strategies such as geo-fencing become more prevalent. However, the public sector is nowhere near the model of corporate network architectures, with dynamic zero-trust capabilities.
- Do more related to **skills, processes and justifying the investmen**t.
- **Automate**, in terms of remote monitoring, patching, password resets, transparency about incidents and triggering alerts for immediate response, applying more sophisticated authentication methods, multi-factor, biometric
- **BYOD** returns to center stage, making BYOD security policies and tools necessary
- **Government cybersecurity policy** for data security, vulnerability, trust management needs to be revised with more people working from home and the need to monitor assets and the location of those assets.
- Over the long term **technology investments**, like creating or buying virtual security services from an operating center, to ensure that applications and data are protected on any device and on any network
- **Rethink security taking into account a hybrid cloud architecture**, ensuring applications that move data across the complex architecture apply the adequate security and encryption

## Short, medium and long term measures

**Phases of activities** that can be applied over the next 6-12 to 18 months:

- In the short term **leverage the existing tools** in a more sophisticated manner
- In the medium term **rethink security policies**
- And in the long term **make the more significant investment into modern technology that can deal with cloud, IoT and the edge**

**Massimiliano Claps**
Research Director, IDC European Government Insights

**We are Alcatel-Lucent Enterprise.**
We make everything connect by delivering technology that works, for you. With our global reach, and local focus, we deliver networking and communications.
On Premises. On Hybrid. On Cloud



Alcatel·Lucent
Enterprise