



SmartCitiesWorld Insight Report

Considerations for building a cyber-resilient city

How to take steps to create comprehensive cybersecurity strategies that consider security-by-design, the human and social aspects of cyberthreats, and threat and attack responsiveness.

In association with

 **PARADOX ENGINEERING**
— MinebeaMitsumi Group —

Written by

Luke Antoniou

Senior Editor,
SmartCitiesWorld

SmartCitiesWorld Insight Reports examine an emerging or growing trend in smart cities, highlighting progress so far and future potential, as well as spotlighting case studies from cities around the world. In this report, we explore how cities can strengthen their cybersecurity postures in the face of growing cyberthreats, and the role that city leaders, city-wide departments and their technology partners have to play.

www.smartcitiesworld.net

Contents

Introduction	3
Embedding technologies created through security-by-design principles	4
The social side of cybersecurity	6
Responsiveness and long-term security	9
Conclusion	12

Introduction

As cities become increasingly interconnected through digital technologies, the importance of strong cybersecurity measures and strategies for urban environments only grows. From traffic management systems and public utilities to healthcare networks and emergency services, cities rely on complex digital infrastructures to function efficiently and safely. However, this growing dependence on technology also makes urban centres prime targets for cyberattacks, which can lead to widespread disruptions, financial loss, and threats to public safety.

This report explores the multifaceted approach required to enhance cybersecurity in cities, focusing on three critical areas: technology, people, and processes. First, the report delves into the adoption of security-by-design and security-by-default by suppliers and why they matter to cities, highlighting the importance of embedding robust security measures into the fabric of urban digital infrastructures from the outset.

The second section addresses the human element, emphasising the need for comprehensive cybersecurity education and awareness among city employees. As the frontline defenders against cyberthreats, employees must be equipped with the knowledge and skills to recognise and respond to potential risks. This section outlines strategies for developing knowledge and fostering a culture of security within city organisations.

Finally, the report examines the processes required for effective vulnerability management and incident response. Establishing the right procedures and organisational structures is essential for identifying weaknesses, managing risks, and responding swiftly to cyber incidents.

City cyberthreats are both increasingly common and sophisticated. In this report, discover the key steps and considerations to safeguard digital urban infrastructure, protect citizens, and maintain the continuity of essential services.



Embedding technologies created through security-by-design principles

Security by design is an approach to developing and deploying technologies that incorporates security principles and best practices from the start, rather than as an afterthought. Security by design aims to ensure that systems are designed with security in mind, following standards and guidelines that reduce vulnerabilities and risks. With the constantly shifting landscape of cyberthreats, it is increasingly important for technologies embedded into urban infrastructure, such as IoT devices and sensors, to be designed with security as a priority, as they could have a direct impact on public safety and service delivery if subject to cyberattacks. By applying security by design, urban technology developers and providers can enhance the resilience and reliability of their systems, protect the privacy and data of citizens, and comply with relevant laws and regulations.

Key benefits of security by design

The key benefits start with proactive threat mitigation. By implementing security-by-design principles, developers aim to mitigate potential threats from the very beginning – during the development phase. While this won't eliminate every risk, those adhering to security by design strive to address around 99 per cent of risks before any code is written or projects are initiated.

Taking a first-hand look at this process, Dario Campovecchi, chief information security officer at Paradox Engineering, explains: "Before we even begin the technical aspects of a project, we start by discussing the goals and expectations with all stakeholders. This includes gathering business requirements and translating them into security requirements right from the first stage of development, not in the middle or at the end. It's crucial to define constraints and limitations in line with the business needs, striking a balance between security and functionality."

Finding that balance is key; neither vulnerability nor business compromise are acceptable outcomes. Campovecchi explains that this balance can be achieved by using risk acceptance criteria to determine which security measures are essential and which might be considered "nice to have" or offer an additional layer of security only when needed. Establishing a baseline set of security requirements comes first, while also recognising that security can sometimes limit functionality. If a city prefers more freedom in their system, it's the responsibility of the provider to clearly communicate the associated risks. Similarly, the reverse is true – if a city wants the most secure solution, they also need to be aware of the constraints and any residual risks.



“A security-by-design approach also naturally ensures increased cyber resilience. Solutions that are secure by design are developed in context with the risks associated with how they operate in different environments.”

“These conversations can feel like a negotiation,” says Campovecchi. “We fully understand that certain aspects of organisational operations for cities are critical, but we have to ensure they recognise the security implications. Take multi-factor authentication as an example: in our perspective, this is non-negotiable and absolutely essential for public infrastructure.”

A security-by-design approach also naturally ensures increased cyber resilience. Solutions that are secure by design are developed in context with the risks associated with how they operate in different environments. If an issue arises – whether in integration with a city’s network or elsewhere – the developer will already know where to look to solve a problem, even if the issue is only caused due to a misunderstanding of logs or incorrect firewall configurations.

Another significant benefit of security by design is cost efficiency. Fixing vulnerabilities at the end of the development process is much more expensive than addressing them early on. By anticipating issues before production and before delivering the product to cities, it’s possible to significantly reduce these costs.

“The security-by-design approach not only helps us respond effectively to issues but also builds trust with those using our solutions,” explains Campovecchi. “They know we’ve put in the effort to anticipate and address potential problems from the start, rather than just reacting and patching systems after issues arise. It strengthens our relationship with them, as they see that we’re committed to delivering secure, reliable solutions.”



The social side of cybersecurity

Cybersecurity is not just a technical matter; it involves a human and social dimension, which is especially relevant for city administrations, who are responsible for managing complex urban ecosystems and delivering public services to citizens. City leaders need to be aware of the potential cyberthreats that can affect their operations, assets, and reputation, and adopt proactive measures to mitigate them.

Additionally, but no less importantly, city leaders need to foster a culture of security among their staff, partners, and stakeholders, ensuring that everyone follows best practices and complies with the relevant standards and regulations. By doing so, city leaders can enhance the resilience and trustworthiness of their smart city solutions, and ultimately improve the quality of life of their communities.


Working with socially-aware vendors

Part of a city's responsibility here is to work with technology companies who also realise the importance of the human element of cybersecurity, promoting it in their own company culture as well as in their product development.

"At Paradox Engineering, we place a strong emphasis on cultivating a security-focused culture within our organisation," explains Dario Campovecchi. "We invest heavily in training our employees, making sure they undergo cybersecurity training every year, whether through classroom sessions or via e-learning platforms. The key is to create continuous awareness, which we reinforce with initiatives like phishing simulations. By running these exercises once or twice a year, we've significantly increased our employees' knowledge and awareness over the past three years."

Internally, strategies like these can prove very effective, but they also present an opportunity to extend a supplier's knowledge to its customers. Vendors whose teams have cybersecurity expertise can share best practices with their end users, like guidelines on password management or other security protocols, to help them strengthen their cybersecurity posture.

“Vendors whose teams have cybersecurity expertise can share best practices with their end users”



“City leaders need to take a proactive stance, and solutions providers can support them by offering expertise, resources, and continuous collaboration”

Passing on knowledge to city leaders

City leaders play a crucial role in this process. They need to champion the importance of cybersecurity within their organisations, ensuring that their workforce is properly educated and prepared to handle cyber threats. This involves not just implementing policies but also fostering a culture where cybersecurity is seen as everyone’s responsibility.

Solutions providers can work in a consultative capacity by offering guidance and resources to help cities build stronger cybersecurity programmes. Campovecchi explains that Paradox Engineering collaborates with public agencies and national cybersecurity centres in order to pass on best practice to cities and help shape cybersecurity programmes for customers more effectively. These kinds of collaborations are particularly important in areas like product testing and infrastructure integration – areas where both vendors and cities need to have always up-to-date expertise with new threats constantly emerging.

One example where this is particularly important is with regards to zero-day vulnerabilities – issues even the original vendors aren’t aware of, where no immediate patch exists. The benefit of being part of a wider support network means that when this happens, vendors communicate these findings with the broader security community to help mitigate the risks. While this type of work doesn’t always make headlines, it’s vital for improving overall cybersecurity resilience. By staying active in the security community and collaborating with public and private entities, these suppliers – and, by extension, their city end users – lead on and contribute to cybersecurity efforts across various fields.

“City leaders need to take a proactive stance, and solutions providers can support them by offering expertise, resources, and continuous collaboration to keep their systems secure and their teams well-informed,” says Campovecchi.



Taking cybersecurity beyond a buzzword

Every city is different in how it establishes a strong culture of cybersecurity, but the key thing is that city governments truly engage with the social side of cybersecurity. It's a changing landscape every day – posturing and saying the right thing isn't going to make city services and infrastructure secure.

Cities who are serious about cybersecurity need to know what they're trying to achieve with cybersecurity measures and follow a clearly defined methodology to get there, taking both a top-down and bottom-up approach, where everyone across the organisation is engaged in the strategy.

City cybersecurity teams must now begin looking beyond the obvious, such as the main documentation and evidence that a solution is compliant to a certain standard. If the supplier is compliant and the city isn't, there's still a very notable weak link in the chain.

There are five key considerations cities should make to strengthen their cybersecurity stance:

- Define your objectives and scope: what are the main goals and priorities of your cybersecurity strategy? What are the assets, services, and data that need to be protected? What are the roles and responsibilities of different stakeholders in the city?
- Assess your current capabilities and gaps: how mature is your cybersecurity posture? What are the strengths and weaknesses of your existing policies, procedures, and tools? How well do they align with the best practices and standards in the industry?
- Develop a roadmap and action plan: based on your objectives and assessment, what are the key initiatives and projects that you need to implement to improve your cybersecurity? What are the timelines, resources, and budgets required for each activity? How will you measure and monitor the progress and outcomes?
- Establish a governance and coordination mechanism: how will you ensure that the cybersecurity strategy is aligned with the overall vision and strategy of the city? Who will oversee and guide the implementation and evaluation of the strategy? How will you communicate and collaborate with internal and external partners, such as suppliers, service providers, regulators, and citizens?
- Build a culture of awareness and resilience: how will you educate and train your staff and users on the importance and best practices of cybersecurity? How will you foster a sense of shared responsibility and accountability for cybersecurity across the city? How will you prepare and respond to potential incidents and recover from them quickly and effectively?



Responsiveness and long-term security

Being able to respond to cyberthreats promptly and effectively is crucial for city services, as they are responsible for delivering essential functions that affect the lives and wellbeing of millions of people.

Any disruption or compromise of these services can have severe consequences, such as endangering public safety, health, and privacy, causing economic losses and reputational damage, and eroding trust in local governments.

City services need to have a robust response capability that can mitigate the impact of cyberattacks, restore normal operations as soon as possible, and learn from the incidents to improve their security posture and resilience.

Developing a comprehensive response plan

The first and most critical step for cities in being more aware and responsive is to conduct a thorough risk assessment, as it is essential to understand where cities stand in terms of identifying potential threats and vulnerabilities. Cities need to know who their enemies might be, which can be uncovered by reviewing the history of attacks on a city, or even looking at national threats. Some countries are more targeted by specific groups, which increases the likelihood of certain incidents. A risk assessment will help cities gain a clear picture of the risks related to their infrastructure and processes.

With this understanding, cities can then define the procedures for detecting, responding to, and recovering from cyber incidents. It's not just about having security tools in place but also about being prepared for scenarios where those tools might fail. Take the recent CrowdStrike issue, for example; many organisations had EDR (endpoint detection and response) systems in place, but when those systems didn't work as expected, there was no emergency plan to fall back on. This highlights the need for comprehensive recovery planning – what do you do when your primary defences fail?

Regular testing of a city's infrastructure and response plans is also crucial. This includes running exercises like phishing to continuously identify vulnerabilities and to test the effectiveness of response plans. These exercises provide real evidence of whether a city's detection mechanisms are working and if its teams are truly prepared. It's not just about having the right tools, but ensuring everyone in the team has the skills and knowledge to respond effectively.

Engagement and communication

Communication is another key element, often overlooked but extremely important. Campovecchi acknowledges that cybersecurity may not be a fun topic for many, but that it's nevertheless critical to communicate to all stakeholders why it matters, what the risks are, and what the potential impacts could be in case of an incident.



“Security is no longer just an IT issue – it’s a management issue, and increasingly, we’re seeing cybersecurity leadership at the top levels of management,” he says. “The impact of a security breach can bring down an entire business, so everyone needs to understand its importance.”

As part of this, there’s a need for a shift in mindset among cities about cybersecurity. The internet may seem like a safe, secure place because threats aren’t visible, but the reality is quite different.

Campovecchi describes cyberspace as ‘a battleground’, explaining: “As in the past when cities built walls for protection, we now need digital fortifications like firewalls, antivirus software, and other security measures. The threats are everywhere, and unlike in traditional warfare, you can’t see your enemies in cyberspace. They could be individuals, organised groups, or even nation-states. Cities need to approach cybersecurity with the same seriousness and vigilance they would any physical threat to their people and services.”

Upgrading and futureproofing

It is crucial that cities invest in technology that is not only innovative and efficient, but also resilient and secure against current and future cyberthreats. This requires a holistic approach that considers the entire lifecycle of the technology, from design and deployment to maintenance and monitoring. Moreover, it requires collaboration and coordination among authorities and technology providers to ensure a shared responsibility and awareness of cybersecurity best practices.

All cities are grappling with legacy systems in some way, the challenge being that many IoT devices often remain in use for a decade or more – thus everything becomes legacy eventually. This means solutions need to be maintained not only for their features but also for their security over a long period of time, putting the onus on cities to find suppliers whose approaches focus heavily on monitoring devices and products in the field.

Campovecchi details Paradox Engineering’s approach to this challenge: “We offer security monitoring through our security operations centre (SOC) specifically designed for IoT. This enables us to keep an eye on any security issues that might arise with our products. The reason we’ve adopted this design approach is that we want our products to be monitored continuously, recognising that what’s secure today may not be secure tomorrow.

“Most cities have their own security operation centres, and our products can be integrated into these systems as well. Our aim isn’t just to provide a product and say that it’s safe and secure – we recognise that continuous monitoring is essential to ensure long-term security.”

One way to deliver on this type of approach is for the vendor to have a baseline set of security alerts in their products. This will allow them to monitor security and manage legacy issues more effectively. Additionally, throughout a product's lifecycle, vendors who take this approach will be able to continue to conduct vulnerability assessments, penetration tests, and security code analysis every year, even if there aren't any new features or software releases. As software and hardware age, new vulnerabilities can emerge, so it's crucial to reassess regularly.

Another potential challenge here comes with cities needing to integrate new solutions with third-party legacy systems. If suppliers have to create integrations with devices not under their control, like city-owned IP cameras, it can lead to situations where those devices have vulnerabilities.

Campovecchi explains how Paradox Engineering has found a methodology for dealing with this situation that still protects the city and the vendor: "Our approach in these cases is to create a sandbox environment or use segmentation to isolate these legacy devices. We apply best practices, like the principle of least privilege and need-to-know, to minimise the impact of any potential compromise on our software.

"Overall, the goal is to ensure that even as these systems age, we maintain security and interoperability while minimising risks. It's a continuous process of monitoring, assessing, and adapting to the evolving cybersecurity landscape."

Threats in a real-world context

During a routine assessment on the IoT network of a customer, Paradox Engineering's cybersecurity team detected a software vulnerability on a connected IP camera.

The device had the potential to become an attractive cybercrime target for three main reasons. First was about privacy: a hacker might be interested in acquiring live images and sensitive information of people living or moving in a certain area. Secondly, the violation might grant visibility on the network infrastructure and pave the way to a wide attack. Last but foremost, the breach might lead to the exploitation of computational power for creating botnet or launch other malicious attacks.

As it dealt with a zero-day vulnerability, no patches or support were available. The customer agreed to remove the IP camera to avoid possible issues and restore the overall security level.

Conclusion

In today's increasingly digital world, cities must take proactive steps to protect their infrastructure and citizens from cyber threats. The foundation of any effective cybersecurity strategy begins with a thorough risk assessment. This process helps cities identify potential threats and vulnerabilities, giving them a clear understanding of where they stand and what risks they face. With this knowledge, cities can develop comprehensive response plans that outline how to detect, respond to, and recover from cyber incidents.

It's not enough to rely solely on security tools; cities must also prepare for scenarios where these tools might fail. Recent incidents, like the challenges faced by organisations relying on Endpoint Detection and Response (EDR) systems, underscore the need for robust recovery plans. Regular testing of infrastructure and response plans is crucial. By conducting phishing drills and other exercises, cities can continuously identify weaknesses and test their preparedness, ensuring that their teams have the skills and knowledge necessary to respond effectively.

Communication is another critical aspect of cybersecurity. It's essential for city leaders to convey the importance of cybersecurity to all stakeholders, emphasising that it's not just an IT issue but a management concern that can have significant business impacts. In today's environment, cybersecurity leadership must be a top priority for city management.

Furthermore, a shift in mindset is necessary. While the internet might seem like a safe place, it's actually a battleground where threats are not immediately visible. Just as cities once built walls for protection, they now need to fortify their digital infrastructure with firewalls, antivirus software, and other security measures. Understanding that cyber threats can come from anywhere, cities must approach cybersecurity with the same seriousness as they would any physical threat to their communities.

About Paradox Engineering and MinebeaMitsumi

Part of MinebeaMitsumi Group, Paradox Engineering designs and implements highly scalable IoT network solutions to control critical public services such as streetlighting, parking management, municipal waste collection, and environmental monitoring. The company has a security operations centre (SOC) and a dedicated team for smart city customers with proven expertise and innovative tools to effectively monitor, support and respond to cyber threats and incidents.

For further information, please [click here](#)



