Photo credit: JC Gellidon

# Smart city resilience: Digitally empowering cities to survive, adapt, and thrive

In the age of the smart city, leaders must adapt their resilience strategy to match their evolving risk profile—otherwise they risk building a smarter but more fragile city.

Paul Nicholas

Senior director,
Microsoft

**City leaders around the world** are abuzz with the profound potential of incorporating smart technologies into everything from their transport infrastructure to water systems to power supply and, of course, to government services. Indeed, smart cities are beginning to come to life in various forms. However, as cities increase their digital dependency, their potential information and communications technology (ICT) attack surface expands dramatically. Cities might be smarter, but without a thorough understanding of cyber resilience, physical and digital crises could be more severe and disruption more sustained than ever before.

Cybersecurity plays a critical role in mitigating shocks and stresses by protecting the confidentiality, integrity, and availability of data and data-enabled infrastructure. However, security alone is not enough. *Cyber resilience* goes a step further by ensuring that ICT systems continue delivering services in the event of a security breach. For cities, cyber resilience can be understood through their capacity for readiness, response, and reinvention. Efforts to build cyber resilience are critical to both surviving and potentially even thriving in the face of cyberattacks or physical disasters.

Indeed, resilience can make a huge difference in the wake of a cyberattack; consider the UK National Health Service, which suffered a ransomware attack last year. But the hospital system had built in enough redundancies, backed up their data, and stayed on top of software updates so that they were able to continue functioning with only a slight delay. Their resilient data and security practices ensured they could continue operations even in the face of an attack.[1] On the flipside, a similar attack on several companies across the globe resulted in losses of millions of dollars due to significant business interruption.

Almost every city is strapped for cash and assets, however, and city managers around the world are struggling to balance investments in cyber resilience with a wide range of other pressing needs. It is essential that city leaders begin to focus less on balancing investments and more on ensuring they are making the *right* investments—ones that are built on a foundation of knowledge about the city's unique threats, priorities, goals, and resources, as well as gaps in critical cyber resilience personnel.

## The first steps toward cyber resilience

Cities will never be 100 percent "secure," nor can they avoid danger entirely. But they can be resilient in the face of a wide range of stresses and shocks by making the right investments, in both the physical and cyber domains, to prepare for crises, react to restore normalcy, and learn from and adapt to the new status quo.

While city leaders tend to have a solid understanding of the physical threats facing them—from earthquakes to terrorism—their understanding of how to mitigate against cyber risk is often spottier. Building cyber resilience requires a profound shift in the way cyber threats are dealt with and assets protected—from focusing on breach prevention to understanding that cybersecurity failures will happen and that quick and efficient recovery capabilities

1 Joseph Cox, "Ransomware targets UK hospitals, but NHS won't pay up," Motherboard, August 30, 2016, motherboard.vice.com.

are needed. In working with cities and governments around the world, we have found the following steps can help public sector agencies—and the many partners on which they depend, from private sector vendors to nongovernmental organizations—ensure that they are ready to respond effectively during and after a crisis.

### 1. Hire a knowledgeable resilience expert to lead the effort.

According to 100 Resilient Cities, an initiative dedicated to helping cities become more physically, socially, and economically resilient in the face of threats, one step cities can take is to hire a chief resilience officer.[2] Most cities today do not yet have the necessary personnel to build an effective strategy. As such, it is important as a first step to hire a manager with relevant experience who will be able to ask the right questions, examine how agencies are currently operating, and design a strategy that takes into account the city's unique situation.

### 2. Identify key threats and assess their potential impact on critical cyber systems and functions.

Every city is different. Understanding the significant and unique cybersecurity threats to a particular city, as well as their potential impact, is vital for ensuring that the city can effectively respond to them. For example, a city that is heavily reliant on bridges for egress will face different resilience questions for its traffic systems than one with more dispersed roadways. This clarity allows the city to identify and plan for the levels of cybersecurity efforts and investments needed.

### 3. Classify and prioritize critical services.

Every city relies on critical services and sensitive information that, if compromised, damaged, or destroyed, would dramatically impact the city's ability to function. Those have to be identified and then prioritized, which often involves tough tradeoffs, but it is essential for the city to be able to effectively respond in a crisis. For example, in the United States, the National Institute of Standards and Technology (NIST) offers authoritative resources, including "Standards for Security Categorization of Federal Information and Information Systems" and the "Protecting Critical Infrastructure Cybersecurity" framework, which can help cities make risk-based security decisions.[3]

### 4. Set cyber resilience goals.

Once threats and critical services are identified, the city needs to set its vision for cyber resilience. On that foundation, it can embark on a collaborative effort to set goals that describe the specific objectives they want to achieve. These goals might include ensuring the city has an effective open-data platform that can provide information to first

2 Michael Berkowitz, "What a chief resilience officer does," 100 Resilient Cities, March 18, 2015, 100resilientcities.org.
3 Both the standards and the framework are available at nist.gov.

responders during emergencies (acute shocks) or helping nonprofits better meet city residents' needs on a daily basis (constant stressors).

### 5. Develop desired cyber resilience outcomes for a crisis.

Unfortunately, we live in a world where it is not a matter of if these events will happen, but when. It's essential, therefore, that cities specify the desired outcomes for the city after a crisis and then identify the capabilities necessary to respond to those events. In the physical world, cities at high risk of earthquakes have established service-level agreements with their citizens—for example, they know what percentage of buildings can be cleared by rescuers within 24 hours. The same such outcomes and agreements should be built for cyber risks.

### 6. Determine the resources needed and define roles and responsibilities.

Finally, the city needs to look at their key threats, priorities, goals, and outcomes and identify what resources are required to deliver the cyber resilience vision. The effort should look across people, skills, technology, and funding, as well as map the responsibilities for actions that need to be undertaken both as a matter of course and in the event of a cybersecurity breach.

## How Rotterdam is taking the lead on building cyber resilience

Only a select few cities have begun to think about cyber resilience as a priority for overall resilience. One of these is Rotterdam, the Netherlands' second-largest city. Taking its inspiration from the municipal motto of "stronger through struggle," Rotterdam developed the first-ever city cyber resilience strategy. Given the central importance of the port to the city's economic well-being, the strategy emphasizes security of port-related ICT assets and cooperation between the public and private sectors to achieve long-term resilience goals. But the plan goes beyond a traditional approach to protecting critical infrastructure and tries to promote more cyber-based innovation, specifically calling on citizens, companies, and organizations to maximize their knowledge and technology use to increase resilience.[4]

Indeed, as cities develop resilience capabilities, they typically become more aware of how many of their resilience efforts depend on well-functioning ICT. In Rotterdam and other cities, managers rely on ICT every day, from making policy decisions to ensuring daily operations run smoothly. That remains true in a crisis. Online services play a critical role in city management but need their own resilience efforts—and this is where cyber resilience comes in. Though it has yet to be tested by an attack, the Rotterdam strategy is the first of its kind and may eventually offer a model for cities wishing to not just survive but thrive in the face of 21st century challenges.

4 Rotterdam resilience strategy: Ready for the 21st century, Gemeente Rotterdam and 100 Resilient Cities, 2016, resilientrotterdamn.nl.

## Cyber resilience is a journey, not a destination

Today Rotterdam is one of the few cities that has embraced cyber resilience; others have begun the journey but still have a long way to go. The novel approach to increasing cyber readiness of cities has only been enabled by recent technological innovation. Moreover, it is not easy to implement, as it requires cities to think, organize, and operate differently. It is even more difficult to measure, given its focus on being prepared for a crisis—which, when it comes, will not play by anyone's rules. Cyber resilience is nevertheless necessary as we continue our march toward a smart city future.

Embracing cyber resilience will not just ensure cities are more secure, it will create opportunities for cities to build comprehensive, long-term strategies that set them on a path toward digital transformation. These, in turn, will promote a culture of innovation, generate new avenues for investment, and contribute to vibrant and economically competitive cities.