Microsoft

CYBER RESILIENCE:
DIGITALLY EMPOWERING CITIES

Authors

J. Paul Nicholas
Jim Pinter

Contributors

Benedikt Abendroth
Robert Arco
Cristin Goodwin
Aaron Kleiner
Laura Ruby

Contents

Executive summary

Our world is becoming increasingly urban. Cities are now home to more than half of the world's population, as well as being economic engines that generate 80 percent of global GDP.

Microcosms of their larger societies, cities face a wide range of complex challenges from persistent stressors, such as high unemployment and violence, to shocks such as earthquakes and terrorist attacks. In response to these challenges, the Rockefeller Foundation launched a seminal effort, 100 Resilient Cities, which provides resources, expertise, and a framework to "help cities around the world become more resilient…" and for people and systems within those cities "to survive, adapt, and grow no matter what kinds of chronic stresses and acute shocks they experience."

As cities plan for resilience, they become keenly aware of how much resilience depends on the smooth functioning of information and communications technology (ICT) in an adaptable technology infrastructure. This cyber resilience is demonstrated by the preparedness of a city's ICT infrastructure for a crisis, its responsiveness, and its ability to reinvent its ICT structure in the face of sustained stress and acute disruptions.

In seeking to develop cyber resilience, a city must determine what it means for their particular city, identify the individuals and services that need to be included in the planning, and create clear goals and objectives. This paper proposes a five-step approach for developing a municipal cyber-resilience strategy:

1. **Identify key threats and assess their impact on critical cybersystems and functions.**
2. **Classify and prioritize critical services.**
3. **Set cyber-resilience goals and objectives.**
4. **Develop desired cyber-resilience outcomes, and identify and test capabilities to achieve them.**
5. **Define roles and responsibilities, and determine resources needed.**

Define roles and responsibilities, and determine resources needed.Increasingly, cities are calling upon the transformative power of technology innovations for solutions to the challenge of building resilience. This paper explores key technologies that we at Microsoft believe will be indispensable to the digital transformation of cities and the advancement of urban cyber resilience: cloud computing, the Internet of Things, big data, machine learning, and artificial intelligence.

The path to cyber resilience is not an easy one. Understanding cyber resilience and developing strategies to address it requires cities to think, organize, and operate differently. This paper aims to provide a concrete foundation for cities as they begin this journey.

Resilience and the modern city

Our world is becoming increasingly urban. According to analyses by the United Nations, more than 54 percent of the world's population currently lives in cities, and by 2050 the population in urban centers is expected to grow to 66 percent—two out of every three people.[1] Our cities are economic engines as well, generating 80 percent of global gross domestic product (GDP) today.[2]

Microcosms of their larger societies, cities confront a wide range of complex challenges that manifest themselves as persistent stressors: high unemployment, inadequate public transportation, violence, water shortages. Cities also face acute shocks: earthquakes, floods, epidemics, terrorist attacks. These drain resources and can prevent cities from making advancements they desire for their citizens, operations, infrastructure, and brand.

So how do cities not only better manage these stressors and shocks, but adapt and thrive? In 2013, the Rockefeller Foundation launched a seminal effort called 100 Resilient Cities (100RC), which provides resources, expertise, and a framework to "help cities around the world become more resilient to the growing physical, social, and economic challenges of the 21st century." 100RC defines urban resilience as the capacity of people and systems "within a city to survive, adapt, and grow no matter what kinds of chronic stresses and acute shocks they experience."

The 100RC effort has focused attention on resilience and the essential role it plays in sustaining the vibrant modern city. Resilience is not a new concept. It has been evolving since the 1990s when it was first thought of as a capability to "fail gracefully" and bounce back. In the contemporary understanding, resilience encompasses preparation for crises and ongoing challenges, whether natural or manmade (readiness), the capability to react to an event and restore normalcy (response), and the capacity to learn from and adapt to the new status quo (reinvention).

Readiness
Response
Reinvention

Resilience encompasses preparation for crises and ongoing challenges, whether natural or manmade (readiness), the capability to react to an event and restore normalcy (response), and the capacity to learn from and adapt to the new status quo (reinvention).

[1] 100 Resilient Cities, accessed 20 February 2017. www.100resilientcities.org/#/-_/

[2] "World Urbanization Prospects, 2014 Revision," United Nations, page 2. esa.un.org/unpd/wup/Publications/Files/WUP2014-Report.pdf

The emergence of cyber resilience

Cyber resilience is the ability of complex cybersystems to continuously deliver the intended outcome despite sustained stress and acute disruptions.

As cities begin to plan to develop resilience, they are becoming keenly aware that their resilience increasingly depends on the smooth functioning of information and communications technology (ICT). City managers rely on this technology and the data it generates to manage and improve day-to-day operations, make decisions, boost efficiency, and control costs. Technology is embedded in our urban DNA.

However, as technology has helped urban centers to thrive, it has also brought new risks. Cities are more and more becoming targets of opportunity because of poor cybersecurity practices, and targets of intent for a range of sociopolitical reasons. A city may first begin thinking about ways to improve cybersecurity and then realize that they have an even bigger challenge—cyber resilience.

Cybersecurity plays a role in cyber resilience, but the two are not equivalent. Cybersecurity is about protecting the confidentiality, integrity, and availability of data, ICT systems, and ICT infrastructure. Cyber resilience is about the ability of ICT systems to continue delivering their intended output in some form, even if cybersecurity is failing or has failed. Cyber resilience does not mean that operations and their supporting infrastructures will not fail, nor that a city is no longer vulnerable to cyberattacks—rather that it can adapt and recover from them. Innovating in a crisis is the true hallmark of resilience.

A growing number of municipal leaders realize that their cities may never be completely secure, so they must build capabilities that are resilient. Cyber resilience is demonstrated by the preparedness of a city's ICT infrastructure for a crisis, its responsiveness, and its ability to reinvent its ICT structure in the face of sustained stress and acute disruptions.

Cyber resilience also requires as much focus on people as on technology. Organizational leadership must foster planning at all levels, setting forward-looking, outcome-oriented goals with clear accountability. Creativity in managerial, operational, and technological approaches is essential. Teams facing the consequences of a cyberattack must be encouraged to take risks, fail fast, learn faster, and maintain a "We can fix this" attitude in the face of adversity. For the long term, investment in research, education, and identification of best practices is also key.

Cyber resilience can best be understood through a city's capacities and capabilities for readiness, response, and reinvention.

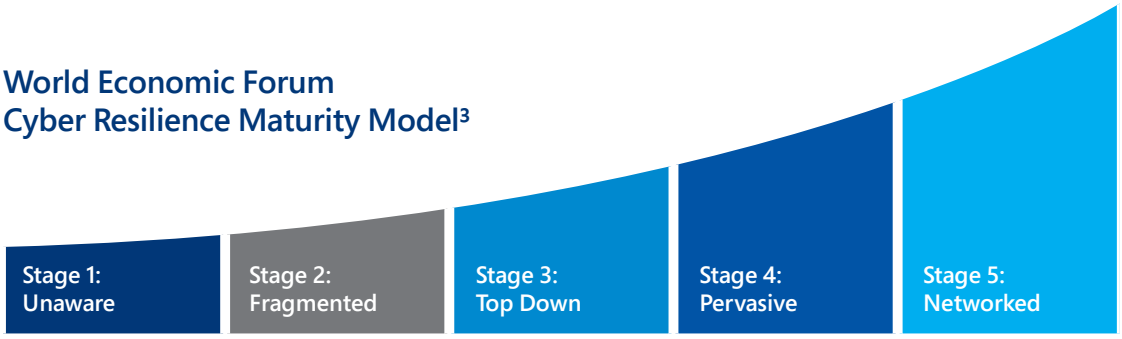
- **Readiness.** To plan for long-term readiness, a city must identify assets, assess and manage infrastructure risk, develop capabilities to respond to and recover from disruptions, and invest in research, education, and practices that contribute to long-term cyber-resilience goals.

- **Response.** Using the plans and strategies set in place during the readiness phase, resilient entities continue to function during a crisis and rebound quickly. A resilient response is also adaptive and flexible—innovating during a crisis is a key element of resilience. If a city is unable to adapt to variables that weren't part of its readiness preparation, it will take longer to regain functionality. The responsiveness of a city to crisis has a profound impact on the reinvention phase.
- **Reinvention.** Learning from and improving on existing plans and strategies is a hallmark of cyber resilience. After a crisis has passed, analysis is key: identifying what was effective and where the response was problematic; developing a plan for improvement; and then implementing that plan. It's important to think beyond short-term gains, and to constantly look to the vision of the city's resilience for ways to reinvent its approach and innovate.

It's often said that "what gets measured is what gets done." This maxim is particularly challenging with cyber resilience, which is rooted in a distributed set of capabilities and capacities that are difficult to measure from a strict quantitative perspective. However, work is taking place to create metrics for resilience in general and cyber resilience in particular.

The World Economic Forum, for example, has created an organizational cyber-resilience maturity model (illustrated below) that can help leaders evalaute where their city lies on a continuum of preparedness, and can serve as a basis for gauging the broad course their city needs to pursue.

World Economic Forum Cyber Resilience Maturity Model[3]



Stage 1: Unaware	Stage 2: Fragmented	Stage 3: Top Down	Stage 4: Pervasive	Stage 5: Networked
The organization sees cyber risk as largely irrelevant, and cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness.	The organization recognizes hyperconnectivity as a potential source of risk, and has lmited insight in its cyber risk management practives. The organization has a sliced approach to cyber risk, with fragmented and incidental reporting.	The Chief Executive Officer has set the tone for cyber risk management, has initiated a top-down threat-risk-response program but does not view cyber risk management as a competitive advantage.	The organization's leadership takes full ownership of cyber risk management, has developed poloicies and frameworks, and has defined responsibilities and reporting mechanisms. It understand the organization's vulnerabilities, controls, and interdependencies with third parties.	Organizations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day-to-day operations. Its people show exceptional cyberawareness and the organization is an industry leader in managing cyber risk management.

Aside from this high-level evaluation, however, cyber resilience for a city can for now be demonstrated by assessing how its specific needs have been addressed by the practical steps taken to build readiness for events, its responsiveness to incidents, and its ability to innovate during and after a crisis.

[3] "Partnering for Cyber Resilience," World Economic Forum, 2012. www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

Developing a city strategy for cyber resilience

A city strategy for cyber resilience must be grounded in and sustained by the city's vision for resilience, and articulate priorities, principles, and approaches to understanding and managing risks.

In some cities, the strategy may center on ensuring the resilience of municipal operations, private businesses, and residents to threats to critical infrastructure; other cities may focus on ensuring access to city data in all crises; still others may prioritize educating newly connected residents and the non-governmental organizations (NGOs) that serve them on how to protect themselves online and how that supports the city's cybersecurity.

Cyber resilience is built through leadership, teamwork, risk taking, trust, flexibility, and a commitment to advance and continually reinvent a city. Based on discussions with urban leaders and resilience experts, the elements below are emerging as central characteristics of a cyber-resilience strategy:

- Cyber resilience in a city is much bigger than the practices of any single entity, so the development and implementation of a strategy requires the involvement of players across the city—city agencies, the private sector, NGOs, citizens.
- Because cities are in a state of constant flux, an effective cyber-resilience strategy must constantly evolve over time to keep pace with that change.
- Cyber-resilience strategies are based on clearly articulated principles that reflect societal values, traditions, and legal principles. For example, if protecting citizen privacy is of extreme importance, it is essential that city strategies—for example, to boost security—do not infringe on this right and value.
- Cyber-resilience is inclusive and leaves no one behind. For example, in emergency situations cities must be able to communicate with and respond to vulnerable populations including people with disabilities, aging communities, and those who do not speak the native language.
- The strategies are based on a risk-management approach, where cities and private sector partners agree on the risks that must be managed or mitigated, or even be accepted.

One of the major challenges to building an effective long-term organizational cyber-resilience strategy and implementation plan is accurately characterizing and quantifying the core capabilities needed. The five-step process below draws heavily on the *Threat and Hazard Identification and Risk Assessment Guide* published by the US Federal Emergency Management Agency (FEMA):[4]

1. **Identify key threats and assess their impact on critical cybersystems and functions.**
2. **Classify and prioritize critical services.**
3. **Set cyber-resilience goals and objectives.**
4. **Develop desired cyber-resilience outcomes and identify and test capabilities.**
5. **Define roles and responsibilities and determine resources needed.**

[4] *Threat and Hazard Identification and Risk Assessment Guide*, Federal Emergency Management Agency, US Department of Homeland Security, August 2013, Washington, DC. www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

1. Identify key threats and assess their impact on critical cybersystems and functions

To ensure that a city can respond to threats to its ICT systems and keep critical government services running, it is vital to understand the significant cyberthreats to the city. But estimating the likelihood of cyberthreats is problematic—there are many malicious actors, as many motives as there are actors, and many different but commonly used attack vectors.

The potential consequences of a cyberattack are also difficult to predict. Network scans or unauthorized system access may be preludes to information theft, a data integrity breach, or disruption of service. Moreover, the complex interrelationships between systems suggest that there may be unanticipated cascading effects, some more severe than the damage originally intended by the hacker. Finally, while some attacks may be obvious (for example, a denial-of-service attack against a critical infrastructure) and generate a quick response, others may be hard to detect. Much has been written about the exfiltration of data from sensitive systems; a more disconcerting scenario might be an alteration of critical data. Not only can this be difficult to detect, but it may be difficult to discern when the data was changed without authority, thus making it difficult to "roll back" to a known good state.

To identify key cyberthreats, estimate their likelihood, and assess their impact, cities may find it helpful to work with partners in the state and federal government, as well as experts in academia and the private sector.

Questions to help you identify key cyberthreats and assess their impact

- What cyberthreats and natural disasters are of primary concern to the city government and the wider community, and how might these affect the city and its residents?
- What is the likelihood of a cyberthreat or natural disaster?
- Does the city's cybersecurity and IT policy include a plan for responding to natural disasters as well as data breaches and other cyberattacks?
- What ICT processes, such as advance threat protection and denial-of-service defenses, are in place to help detect, prevent, and respond to a cyberattack or natural disaster?
- What cross-agency coordination teams exist to ensure a common awareness of threats and possible impacts, and how often do they meet?

---

2. Classify and prioritize critical services

Every city relies on certain critical services and sensitive information which, if compromised, damaged, or destroyed, would dramatically impact the city's ability to function. Prioritizing which services to protect involves tough tradeoffs. Although it is tempting to identify all services and assets as high priority, focusing on only truly essential services helps ensure that cities will be able to respond.

To take on this challenging task, cities must first identify critical services and assets. Municipal agencies often have a list of these, which can be a good place to start. With this list in hand, cities can then define and implement a clear framework for classifying data and services (including those operated by third parties) as high, medium, or low impact. The National Institute of Standards and Technology (NIST) offers one such framework: *Standards for Security Categorization of Federal Information and Information Systems* (csrc.nist.gov/groups/SMA/fisma/categorization.html).

Once services are classified, prioritizing them must be grounded in a solid understanding of the inner workings of each service and how it is connected to and dependent on other services. For the deepest insight, engage the managers and employees who implement the services, and the city residents who rely on them. It can also be useful to research how other cities have prioritized their services.

It may be that one service is important to a very large number of residents or fundamental to the smooth functioning of the city—such as working traffic lights or clean water. Another service may seem important, but if an alternative can be substituted, then it may not be as high a priority. For example, if the city website were down, social media could fill the need for informing residents.

As cities prioritize services, they also need to look at security for those services. If a certain service is a high priority, security protections should be commensurate with its importance to the city. Furthermore, If services share a common priority, they can also share the same Protection Profiles. The NIST *Framework for Protecting Critical Infrastructure Cybersecurity* (www.nist.gov/cyberframework) is an authoritative resource that can help with making risk-based security decisions.

As a side note, this process of classifying and prioritizing services has other benefits in addition to building cyber resilience. It can reveal how systems and their dependencies have changed or evolved over time, and it may uncover changes in business processes, as well as the consolidation and simplification of ICT investments.

Questions to help you classify and prioritize critical services

- What critical services does the city need to protect most and recover first?
- Who is responsible for each of these critical functions?
- How long can certain services be offline or interrupted before they become critical—1 hour, 5, 24, 72?
- Where are the city's operations physically located and which can be transferred to the cloud to better withstand a crisis?
- Do cybersystems have a documented recovery plan and how often are they tested?
- Is there a city-wide risk acceptance process that properly documents expectations and agreements?

---

3. Set cyber-resilience goals and objectives

Before a city can set goals and objectives, municipal managers and key stakeholders must have a clear understanding of the city's vision for cyber resilience—a vision that reflects societal values, traditions, and legal principles.

On that foundation, the city can embark on a collaborative effort to set goals that describe a high-level desired outcome or capability, and supporting objectives—activities that will help the city achieve those goals. We recommend linking the critical services that the city has prioritized to the cyber-resilience goals of the city, following this general guidance:

- Start small and simple, and build momentum. Set goals and objectives that are not overly complicated and that the city has the capability to implement.
- Ensure broad representation—from city managers and employees to the wider community—so that everyone has a stake in understanding the resilience goals and objectives that they will be responsible for implementing together.
- Be inclusive. Ensure that your ICT plans address the needs of all citizens including vulnerable populations, aging communities, and people with disabilities.
- Develop goals and objectives that are flexible enough to accommodate the inevitable changes in municipal organizations and in technology.

Questions to help you set cyber-resilience goals and objectives

- Do these goals and objectives align with the city's needs and priorities?
- Can the city's IT department and ICT architecture meet these goals and objectives?
- Can the city leverage partnerships with private companies to help meet its cyber-resilience goals and objectives?
- Recognizing the role of NGOs in supporting city residents, what does the city need to do to prepare them for increased cyber resilience?
- Has the city set up ways to communicate with and deliver services to vulnerable citizens should key infrastructure systems be compromised?
- Has the city established a well-understood strategic cybercommunications and coordination capability that brings together incident response, legal, public relations, public safety, and other relevant stakeholders?

4. Develop desired cyber-resilience outcomes and identify and test capabilities

Cyberattacks or natural disasters do not cause problems just for IT departments; increasingly they deliver physical disruptions as well—for example, creating political and social unrest or physically destroying hardware and data.

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 or in response to ongoing stress, and then identify the capabilities—whether existing or waiting to be funded or created—necessary to respond to those events and successfully deliver those outcomes.

As described in the FEMA guide, "Desired outcomes describe the timeframe or level of effort needed to successfully deliver core capabilities. Capabilities are only useful if communities can deliver them in a timely and effective manner."[5] When it comes to cyber resilience, success for a city can be defined either as the delivery of capabilities within a certain timeframe or in terms of percentages of critical functions restored.

For example, in the event of a sophisticated cyberattack against a city's ICT infrastructure, a city may determine the desired outcome to be repairing a certain percentage of that infrastructure. If reports surface of damage to its fiber cabling, a city may set a short timeframe to assess the damage, and then allocate more time to make the full repairs. If hacking damages traffic control sensors, the city can specify a rapid evaluation and repair of the vulnerabilities.

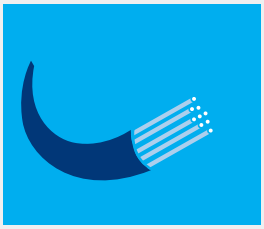
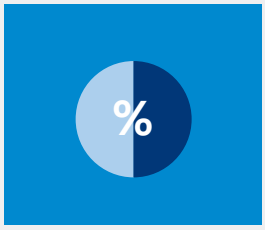
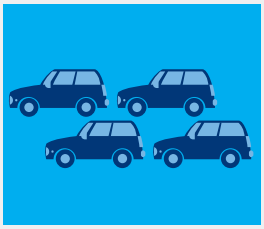
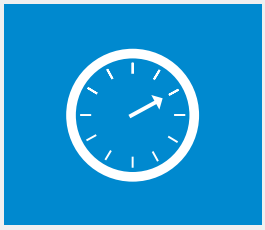
Once these outcomes have been defined, they need to be reviewed and tested to ensure that the city has the capability to deliver them within the timeframe or to the percentage that have been specified.

Questions to help you develop desired cyber-resilience outcomes and capabilities

- If the city lost all IT support for public safety and law enforcement during a major crisis, how quickly could it resume minimum critical ICT functions and meet your defined goals?
- What expectations do city stakeholders have for the city's time to recover key operations?
- How can the city leverage the cloud to manage and scale response in a crisis? What planning is needed to ensure that operations can be transferred to or managed from the cloud?
- Has the city invested in building key applications to modern standards that can be transferred to the cloud as needed?
- Does the city have processes in place to build and improve capabilities?
- Does the city have budget and other resources to build its capabilities?

[5] *Threat and Hazard Identification and Risk Assessment Guide,* FEMA, page 12.

Specifying desired outcomes and identifying capabilities

	Identify impact	Specify desired outcome	Capability to be developed
Time-based outcome	 Reports of outages over 100 miles of fiber cabling.	 Restore fiber connections within 24 hours.	Assess fiber cabling within 5 hours and repair within 24 hours.
Percentage-based outcome	 Sophisticated cyberattack immobilizes part of the city's ICT infrastructure.	 Restore 50 percent of the ICT infrastructure within 48 hours.	Evaluate damage within 2 hours, and repair within 48 hours.
Time-based outcome	 Traffic control sensors were hacked, resulting in gridlock.	 Restore traffic control within 2 hours of the attack.	Evaluate compromise within 30 minutes. Repair vulnerabilities and regain control within 2 hours of attack.

5. Define roles and responsibilities and determine resources needed

To best determine the resources needed for cyber resilience, start with the functional understanding of the critical city services that was developed in Step 2. Now consider this through the lens of resources required—people and skills, technology, and funds.

Starting with a matrix of key stakeholders and technology owners, clearly identify who is responsible for each functional area when responding to a crisis, assign and clarify specific responsibilities for those roles, and determine what resources are available to them. Knowing this in advance will cut down on response time and help clarify the best course of action for addressing the problem.

Defining roles can be a difficult task—role assignments may need to cut across traditional lines of authority, with accountability and responsibility shared among municipal services. Without clarity, however, in a crisis there could be conflict over who is to supposed to do what. Two leaders could compete to claim responsibility; alternatively, there is the possibility of no action at all because each team believes the other is tackling the problem. The solution is to assign a lead who would oversee and coordinate the response across all involved services.

For example, let's say that a city's transportation website crashes and citizens can no longer access bus routes and times. It is vital, of course, to know who within the department of transportation is responsible for resolving the issue. But this problem could very well impact other teams—the mayor's office, communications team, IT center. So during the process of defining roles, the city would identify a lead who would coordinate the response of all teams involved. Additionally, the city would need to ensure that it has other resources in place—for example, social media where citizens could receive updates from city officials, or even a backup website with bus schedules.

This process of delineating responsibilities will also raise questions about the funds and technology available—and where these may be inadequate. Cities need to identify gaps in both people and technology resources that may limit their ability to respond, and make the allocation of those funds part of the regular budget process.

Questions to help you determine resources and define roles and responsibilities

- Who is ultimately responsible for the cyber resilience of the city and execution of its strategies?
- Does the city have a process to engage infrastructure providers, businesses, and residents to discuss its needs and consider if there may be joint investments that could improve its cyber resilience?
- Who owns and maintains the ICT risk registry, and does it take into account both the physical and ICT infrastructure?
- Where should the city spend its next resilience dollar?
- Is there a cyber-resilience budget to help executives understand what investments are being made and what additional investments may be needed?
- If migrating certain cyber-resilience functions to cloud-based systems has saved money, where should the savings be applied?

Digital transformation enables cyber resilience

Over the past decade, significant technology advancements have helped cities increase their productivity, improve communication, and innovate in support of their growth and prosperity. increasingly, cities are also calling upon the transformative power of digital technology for solutions to the challenge of building resilience. This digital transformation can change how cities understand, monitor, and manage environmental and operational challenges, and help accelerate the journey of cities to become more resilient.

Through digital transformation, cities will:

- **Better engage and empower residents and understand their needs.** Business intelligence plays a critical role in analyzing massive amounts of data (*big data*) to recognize patterns of sentiment and behavior in an urban setting. For example, the city of Boston implemented Adopt-A-Hydrant (www.adoptahydrant.org/), which maps fire hydrants across the city and encourages residents to take responsibility for shoveling out a hydrant close to them after it snows.
- **Empower city employees.** Knowledge and insight exist within a city's infrastructure, just waiting to be found. For example, data is available about how employees work—desktop computers or laptops and other mobile devices; in the office, out in the city, or from home. Based on an analysis of these habits, cities could design systems that support a mobile workforce, thereby reducing cost and improving productivity.
- **Optimize city operations.** Digital technology now enables cities to understand problems in new ways, make predictions, and adjust as needed, accelerating responsiveness to inefficiencies and other issues. For example, city traffic operators can view traffic in real time, and adjust traffic signals to clear bottlenecks and speed the flow of traffic in congested areas.
- **Transform city services.** Cities can create connected services and generate insights to unlock new business models for municipal departments and spark economic opportunity in the city. For example, the Belgian municipality of Ottignies-Louvain-la-Neuve deployed Opisense, an Azure IoT Hub and Power BI solution, to monitor energy usage in its buildings and take corrective action when abnormal usage was observed. The result? Reduced energy usage by more than 25 percent in monitored buildings.

There are a few key technologies that we believe will be indispensable to the digital transformation of cities and the advancement of urban cyber resilience:

- Cloud computing
- The Internet of Things
- Big data and machine learning
- Artificial Intelligence

Cloud computing

One of the greatest advancements in cyber resilience (and organizational resilience overall) has been the creation of cloud computing—moving data and services to the cloud. By 2025, most of the data created in the world will move through or be stored in the cloud at some point. Cloud computing not only offers elastic, secure, and cost-effective technology solutions, but it can also support cyber resilience—it is designed for high availability and resilience in the event of a failure through improved security and geographic replication of data.

Cloud computing has enabled cities to increase the agility and efficiency of their operations, reduce operating costs, boost the productivity of their workers, and enhance the resilience of their ICT infrastructure.[6] City data can be stored and secured using the latest software and hardware; something that would have cost thousands of dollars in the past is now provided at a fraction of the cost. Furthermore, because resources are elastically provisioned, they can quickly scale, and cities pay for computing resources only when they need them. This can be particularly helpful for government functions such as processing tax returns or deploying snow removal equipment that experience predictable spikes in usage and capacity.

Cloud computing can improve security because it transfers some responsibility for managing ICT to the cloud service provider (CSP). Depending on the service model, cloud providers may manage not only datacenter security but also network controls, identity and access controls, and patching. Large CSPs also have visibility into threats worldwide and the ability to rapidly protect their entire environments, with specialists dedicated to specific security threats. They also see providing robust security as a competitive differentiator and therefore invest heavily in it, often devoting substantially more resources to improving ICT security than any city government could afford.[7]

Cloud computing can use geographic replication to protect data and services. With centralized data storage, management, and backups, data recovery in response to local disruptions can be faster and easier. Large CSPs build databases in many locations around the world, which enables them to host relevant data or services in regions unaffected by local or regional emergencies. Therefore, if a city loses access to its on-premises servers in a crisis, cloud providers can continue to safeguard data and support essential government services. In fact, many CSPs back their assurances of data availability by offering a service level agreement that provides 99.99 percent uptime to their customers.

Best practice: Cyber resilience for Estonia through cloud computing

In 2014, Estonia conducted a pilot project with Microsoft to determine the benefits of moving two government services—the president's website and the country's law registry—to the public cloud. The study centered on whether cloud capabilities would help ensure digital resilience for Estonia in the event of a natural disaster, civil unrest, or attack by another country.

---

[6] *Value of Cloud Security: Vulnerability,* Leviathan Security Group, 2015. www.leviathansecurity.com/s/Value-of-Cloud-Security-Vulnerability.pdf

[7] *Value of Cloud Security.*

The pilot found that many of Estonia's government registries were in digital form, with no hard copy or digital backup. In addition, the content was stored only within Estonia's borders, with no ability to move it elsewhere in a crisis. The pilot determined that moving data to the public cloud could help Estonia achieve the digital continuity required to increase the security and resilience of its infrastructure, data, and services.

The Internet of Things (IoT)

Because of falling hardware costs, software advances, proliferating connectivity, and scaling cloud solutions, we have seen a significant growth in the Internet of Things—the connection of everyday objects to the Internet. It is estimated that 50 billion devices, including those in cities, such as streetlights, parking meters, and traffic cameras, will be connected to the Internet by 2025.

As IoT deployments mature, the sensors in Internet-enabled devices and the systems that process the real-time data they send will enable more effective and efficient decision-making that can dramatically improve urban resilience. They may provide updates about municipal operations that offer predictive—and even preemptive—prescriptions for maintenance of municipal infrastructure, including equipment, traffic cameras, or streetlights.

In San Diego, California, for example, city officials have started to modernize their traffic light systems by installing video and traffic sensors, along with bike and pedestrian counters, on all 1,540 traffic signals. The data those sensors deliver to a central control will enable the city to adjust the signals based on peak use, and substantially reduce traffic congestion.

Best practice: The Internet of Things helps increase the reliability of ThyssenKrupp Elevators

ThyssenKrupp Elevators turned to the IoT and machine learning to improve their maintenance predictions and help ensure greater reliability of their elevators. ThyssenKrupp fed the data derived from their elevators and sensors through the Microsoft Azure Machine Learning service, which created dynamic models that predict when a part or feature will need to be replaced, and alert technicians before they become a problem. This has significantly improved the reliability of their elevators, giving the company a competitive edge and cutting operations costs.

Artificial intelligence gives computers the ability to reason, communicate, and perform with humanlike intelligence, skill, and agility.

Big data and machine learning

With the significant growth in IoT and cloud computing, cities are increasingly drawn to the use of big data and machine learning. Cities, whether they realize it or not, already have a significant amount of data available to them from their existing infrastructure—traffic logs, maintenance requests, citizen feedback—that could, through the use of machine learning, dramatically improve municipal functions and build resilience.[8]

Big data refers to extremely large volumes of both structured and unstructured data that can be analyzed to reveal trends and patterns, often relating to human behavior. The use of big data can open new insights into city performance as well as patterns related to how citizens interact with city services. For example, Barcelona in Spain has used big data insights to change the distribution of bicycle rentals across the city to make it easier for people to connect to buses and trains, and to improve traffic flow.[9]

Machine learning is the practice of feeding data from a wealth of sensors, devices, and other city assets into predictive models, and then using the power of the IoT to feed those insights back to the systems and people who can make predictions and take action. For example, energy companies run the data they collect from connected sensors and smart meters through machine learning software to help grid operators balance and predict supply and demand to prevent blackouts.

Best practice: Oakland Athletics win with big data

Perhaps you've seen the 2011 movie "Moneyball," the true story of how the Oakland Athletics' Billy Beane and Paul DePodesta (played by Brad Pitt and Jonah Hill) used big data to field a competitive baseball team despite a low budget. They used statistical analysis of a vast array of player data, including hitting, fielding, and pitching, to choose the players for a team that would compete most effectively against the other 29 Major League Baseball (MLB) teams in the United States. The result: the most consecutive wins by a team in MLB history, a record that still stands today.

This is also a great example of the enduring power of big data. Because of the Athletics' success, all 30 MLB teams today use big data to ensure that they are fielding winning teams while spending as little as possible.

Artificial intelligence

Artificial intelligence (AI) gives computers the ability to reason, communicate, and perform with humanlike intelligence, skill, and agility. AI is not a new technology, but its practice has grown significantly over the past few years by harnessing the explosion of such technology advancements as big data, improvement in AI algorithms, and the ability to process data more quickly. Many still view AI with concern, fearful that it will one day take over or replace jobs. But at Microsoft, we believe that AI can help people, not replace them, and be used to enable collaborative interactions between people and machines, as well as to support all kinds of organizations, including cities.

[8] James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, Dan Aharon, "Unlocking the potential of the Internet of Things," McKinsey Global Institute, June 2015. www.mckinsey.com/insights/business_technology/the_Internet_of_things_the_value_of_digitizing_the_physical_world

[9] Iain Jawad, "World's Top Global Mega Trends to 2025 and Implications to Business, Society and Cultures," (paper presented at IPA Forum 2014, Helsinki, Finland, June 9–10, 2014). www.investinbsr.com/ipaforum/wp-content/uploads/Iain-Jawad-IPA-Forum-2014-Presentation.pdf

So how can AI help a city become cyber resilient? To achieve cyber resilience, cities must constantly test, learn from, and improve their systems, operations, and organizational resilience. Microsoft is advancing the state of the art in machine intelligence and perception by preparing computers to understand what they see, communicate in natural language, answer complex questions, and interact with their environment.

Best practice: Breaking language barriers with Skype Translator

At Microsoft, teams have worked for over a decade to create a technology that can help break down the language barrier: Skype Translator. The service relies on deep learning, a type of artificial intelligence that involves training artificial neural networks on lots of data (recordings of speech, in this case) and then making inferences about new speech. In use, Skype Translator comes up with a few text candidates in the first language, chooses the top candidate, translates the text based on previous translations, and provides a speech recording of the translated text. With user feedback, it gets better over time. Through this near–real-time speech recognition, people can now have conversations in many languages translated into their native tongue with almost no delay.

Skype Translator can be helpful in polyglot cities like Rotterdam in the Netherlands, where citizens have come from more than 170 different countries. This situation can create a "Babylon effect" within a city, where language barriers prevent citizens from accessing services they need or taking jobs. Using Skype Translator, a city like Rotterdam could remove this obstacle and provide these services, as well as make it possible for people who don't speak Dutch to take certain jobs, turning what once was a challenge into a municipal asset.

Conclusion

The path to cyber resilience is not an easy one. Understanding cyber resilience and developing strategies for it requires cities to think, organize, and operate differently.

Cyber resilience is an emerging discipline that only a handful of cities have begun to undertake. As cities begin to consider cyber resilience and create plans, they must determine what it means for their particular city, identify the individuals and services that need to be included in the planning process, and create clear goals and objectives. Through this work, cities can build long-term strategies that prepare them and their people for the future, and in turn promote a culture of innovation, generate economic opportunity, and contribute to a city that is more economically competitive.

We hope this paper provides some concrete strategies for cities to explore as they begin their journeys to cyber resilience.

Helpful Resources

100 Resilient Cities.
www.100resilientcities.org/#/-_/

"Partnering for Cyber Resilience," World Economic Forum.
www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

Threat and Hazard Identification and Risk Assessment Guide, Federal Emergency Management Agency, US Department of Homeland Security.
www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

Standards for Security Categorization of Federal Information and Information Systems, NIST.
csrc.nist.gov/groups/SMA/fisma/categorization.html

Framework for Protecting Critical Infrastructure Cybersecurity, NIST.
www.nist.gov/document-3766

Transforming Government: Cloud policy framework for innovation, security, and resilience, Microsoft.
aka.ms/cloudsecurityprinciples

Developing a National Strategy for Cybersecurity, Microsoft.
aka.ms/national_cybersecurity_strategy

Developing a City Strategy for Cybersecurity, Microsoft.
aka.ms/city_cybersecurity_strategy

Microsoft