Microsoft

DEVELOPING A CITY STRATEGY FOR CYBERSECURITY

Foundations for security, growth, and innovation

CRISTIN FLYNN GOODWIN
J. PAUL NICHOLAS

July 2014

Contents

Executive summary

With the growing number of cyber threats in today's complex security environment, a principled cybersecurity strategy is critical for managing risks. To this end, Microsoft helps cities take proactive steps to protect their information, systems, and infrastructures. A secure city can be confident that it is better positioned for opportunity and growth. As a global company, Microsoft has helped hundreds of cities address cyber risk. This paper contains recommendations, based on years of experience, that can help city leaders to develop or improve their cybersecurity strategies and to fit this work within other transformational programs aimed at increasing resilience.

Introduction

Every region of the world is experiencing rapid urbanization. More than 50 percent of the world's population lives in urban areas. By 2050, that number will grow to nearly 70 percent, or more than 6 billion people.[1] While some areas will experience more intense urbanization than others, for example India will almost double its urban population between 2011 and 2031[2],dramatic urban growth has become a truly global phenomenon.

As a city leader, it's hard to imagine this extraordinary rate of growth in such a short period of time. City resources are stretched, planning is hampered by economic realities, and the critical challenges of today, such as aging infrastructures, low employment rates, and transportation demands, require everyone's attention.

What is cybersecurity? Cybersecurity means different things to different people. For a city, cybersecurity is the protection of information, systems, and infrastructure vital to the city's operation and to the stability and the livelihood of its people.

Connected cities

Despite these challenges, rapid urbanization continues, and, along with it, a web of interconnected systems. By 2020, more than 50 billion objects are expected to be connected to the Internet[3] as an Internet of Things, which defines a world where just about anything can be virtually connected. People are also racing toward this same level of connectivity. The Microsoft Cyber 2025 Model[4] predicts that there will be 4.7 billion Internet users in 2025, with nearly half coming online between 2012 and 2025, almost entirely from emerging economies. Many of these connections will come from mobile broadband, through devices such as phones and tablets.

Resilience

So how does a city boost resilience in the face of both urbanization and a complex cyber-ecosystem? There are a number of factors to help a city "survive, adapt, and grow."[5] From a technology standpoint, these include:

1 United Nations, Department of Economic and Social Affairs, Population Division, World Urbanization Prospects: The 2011 Revision. http://esa.un.org/unpd/wup/CD-ROM/Urban-Rural-Population.htm

2 Building and managing intelligent cities in India. Accenture. http://www.accenture.com/in-en/Pages/insight-building-managing-intelligent-cities-india.aspx

3 Dave Evans, The Internet of Things: How the Next Evolution of the Internet is Changing Everything (Cisco, April 2011), 3, PDF, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

4 Microsoft Cyberspace 2025, http://www.microsoft.com/security/cybersecurity/cyberspace2025/#chapter-1

5 The Rockefeller Foundation, 100 Resilience Cities, What is Resilience? http://100resilientcities.rockefellerfoundation.org/resilience

91%

of breaches are attributed to an employee clicking a link.

- **Enabling greater Internet access for citizens**

  Internet connectivity supports a city's resilience by providing paths for communication, increasing education, and stimulating economic growth. According to the International Telecommunications Union (ITU), 78 percent of homes in developed countries have Internet access, while mobile-broadband penetration is at 84 percent. Developing countries will see the most mobile growth in 2014, with 55 percent of all mobile-broadband subscriptions.[6] Ensuring that cities can find creative and innovative ways to work with Internet providers to promote Internet access from within the city will help drive growth.

- **Expanding the use of smart technology in core services and physical infrastructure**

  The use of smart technology, such as big data analytics and mobile applications, to improve services is a hot topic for cities. One such game-changing application is Uber, a ride-sharing service managed through a mobile app. With innovations like this, cities are looking at ways to balance the benefits for citizens against smart regulation and citizen safety. Using smart data has also benefited cities through citizen services and infrastructure improvements. For the 2012 Olympics, the City of London improved its transportation infrastructure by making more of its data available to citizens; information about service disruptions to the underground system and real-time bus arrival times were made available through smartphone apps, allowing people to efficiently navigate the city.

- **Openly sharing information between departments, private sector, and other cities**

  Information-sharing helps to increase innovation and to decrease security threats. Open communication channels should be developed between city departments, local companies, and other government entities.

- **Developing robust cybersecurity policies and procedures**

  New systems and apps are only as effective as they are safe. A cybersecurity strategy lays the groundwork for thriving ICT innovation, provides the backbone for a resilient city, and can draw upon national standards to help simplify procedures.

How can Microsoft help?

Microsoft draws on years of experience dealing with cyber threats around the world to help cities develop cybersecurity strategies. Each month, the company receives threat information from more than 600 million systems in more than 100 countries and regions. Microsoft also works closely with governments, companies, and individuals and has a first-hand view of how organizations manage risk within their environments.

Leveraging this vast knowledge of threats and direct experience with city leaders, Microsoft has created a principled approach to help cities design and implement their cybersecurity strategies. This approach includes six steps, each with specific recommendations to guide strategy development. In the appendix, recommendations.

6 ITU, ITU releases 2014 ICT figures, http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.U4feMKxOXbg

Creating a city strategy for cybersecurity

On a national level, policymakers are grappling with principles, policies, and programs to improve cybersecurity. Cities are now becoming part of this discussion because of the rapid urbanization happening around the world. However, cities have practical security needs that can't wait for international or national politics. They need ways to prioritize risks and to assign roles and responsibilities for key aspects of cybersecurity within their own infrastructures. Cities also have to balance cost, existing and legacy systems, and effective administration of new programs and systems. A cybersecurity strategy can help a city get started immediately to enhance the integrity, availability, manageability, and confidentiality of city information, citizen services, and business operations.

Characteristics of an effective cybersecurity strategy

An effective cybersecurity strategy is continually reevaluated in light of new threats, technology advancements, and city transformation. It reflects societal values and legal principles so as to not alienate citizens or infringe on their privacy and values. It is based on a risk-management approach, where city leaders and other stakeholders agree on the risks to be managed, mitigated, and even accepted.

Characteristics of an effective cybersecurity strategy
Clearly articulate a city's cybersecurity priorities, policies, and programs
Define goals, milestones, and metrics to measure and communicate progress
Give citizens and organizations an opportunity to provide input
Educate citizens about cyber risks and mitigation approaches
Ensure appropriate resources
Specify the roles of each city agency and other groups involved

Implementing a principled approach to cybersecurity

At its heart, a cybersecurity strategy should reflect the values of a city. It must have a clear set of principles to help frame decisions about how to identify, manage, and mitigate cybersecurity risks in a way that balances civil rights and privacy, costs, and other priorities in today's push toward cloud- and mobile-connected cities. Microsoft recommends six cybersecurity principles to guide a city's strategy:

In 2013,

13.1 million

consumers suffered identity fraud.

Cybersecurity strategy principles	
	Risk-based. Assess risk by identifying threats, vulnerabilities, and consequences, and then manage it through mitigations, controls, costs, and other measures.
	Outcome-focused. Focus on the desired end state (rather than prescribing the means to achieve it), and measure progress toward that end state.
	Prioritized. Adopt a graduated approach to priorities, recognizing that disruption and failure are not equal among critical assets or across critical sectors.
	Practicable. Optimize for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors.
	Respectful of privacy and civil liberties. Include protections based upon the Fair Information Practice Principles[7] and other internationally-accepted privacy and civil liberties policies, practices, and frameworks.
	Nationally and globally influenced. Integrate national and international standards to the maximum extent possible, keeping harmonization in mind.

7 Fair Information Practice Principles, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf; http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

Understanding the cyber threat landscape

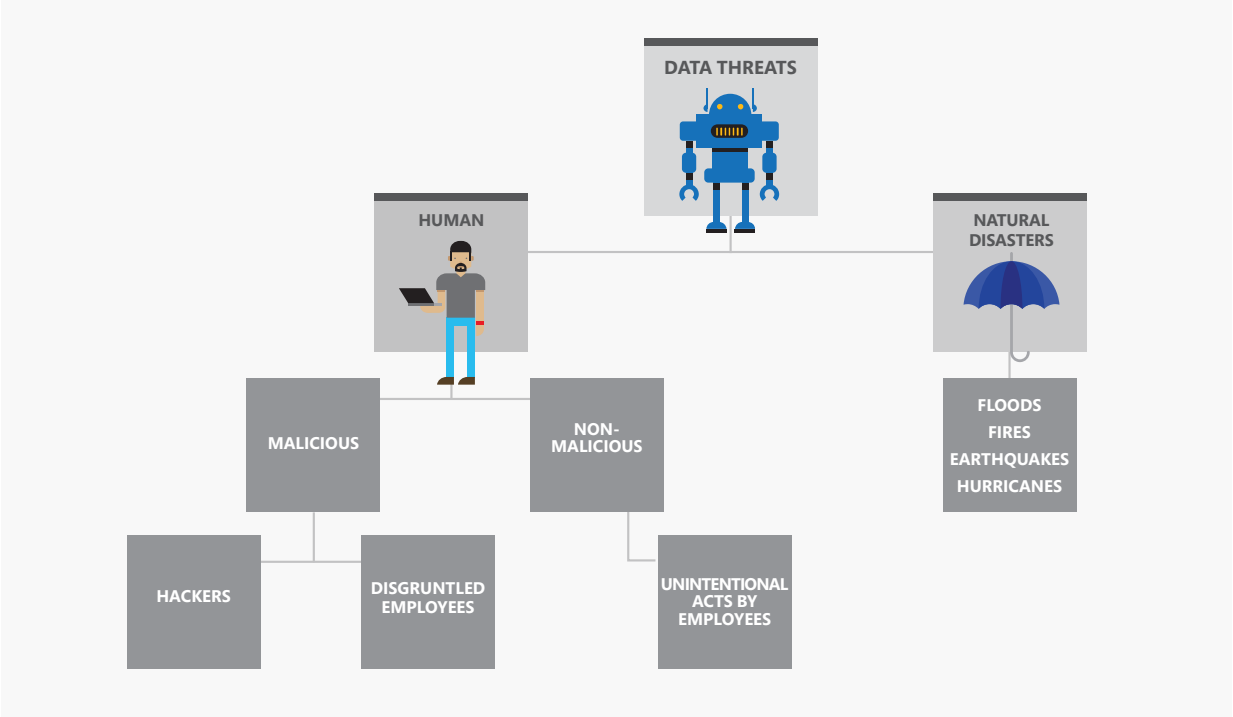
The type of cyber threats facing cities has grown more complex and includes everything from malicious software and spam to online fraud and terrorist activity. Cities trying to grasp the cyber threat landscape can benefit from threat modeling to help them understand what they are trying to protect (assets) and who they are protecting those assets from (threats). A threat model inventories assets and threats, determines the likelihood that assets will need protection, looks at a city's ability to do so, and determines the consequences of inactivity. Just as software architects uncover technical vulnerabilities during threat modeling, following this approach would allow city leaders to identify and mitigate potential security issues early, while they are still relatively easy and cost-effective to resolve. Specific guidance for threat modeling can be found on page 12 of this paper.

To ensure threat modelling is effective, city leaders should prioritize their engagement and first look at the most likely areas in which cyber threats can impact cities.

Data

Information is a critical part of a city's ability to maintain services and connect with citizens. Health records, police reports, and business taxes all contain data that should be protected. In the wrong hands, this data can be manipulated to inflict damage on individuals and institutions. While use of smart data is vital to improving public services, it also means that there is an increasing amount of information at risk.

Threats to data are primarily human-driven, although data loss due to natural disaster is a possibility. Human threats may be non-malicious, such as the unintentional downloading of infected software onto city computers. Conversely, they can be malicious,[8] such as an insider stealing or corrupting data or a hacker disrupting services.



8 2012/2013 The South African Cyber Threat Barometer, http://www.wolfpackrisk.com/wp-content/uploads/2012/10/SA%202012%20Cyber%20Threat%20Barometer_Medium_res.pdf

Two recent examples shed light on the vulnerabilities of city data. In late 2013, a flash drive was stolen from a Milwaukee, Wisconsin, contractor. The drive contained the unencrypted Social Security numbers and personal information of 6,000 city employees.[9] A few months later, in Johannesburg, South Africa, a security glitch was identified that exposed customer rates and services invoices to potential fraud because basic security measures had not been implemented on the system[10].

A people-driven threat assessment of data is integral to a city's cybersecurity strategy. It should help define how city services collect and use data, how citizens are accessing and using it, and how privacy can be assured in the process.

Systems

A city's digital systems are vital to its continued operations. School systems use online tools to facilitate learning and increase skill development. Law enforcement's online systems help ensure that citizens are safe and protected. Emergency communications systems are crucial during storms or medical emergencies. When these systems are compromised, city services are interrupted and citizen safety is at risk. As with threats to information, systems may be compromised by both malicious and unintentional actions.

In 2012, a group of hackers, known as the UGNazi collective, attacked the New York City and District of Columbia websites, knocking them offline.[11] More recently, hackers targeted the Australian Federal Police website with a DDoS attack, also taking it offline.[12] During Typhoon Haiyan, power and communications systems were disabled, in some regions, for months. As a city considers a possible range of threats and threat actors, it is important to think about city systems and define which are critical to city services and which help ensure appropriate resilience and reliability for those services.

Infrastructure

Critical infrastructure is generally defined as the key systems, services, and functions that, if disrupted, would have a debilitating impact on public health, safety, commerce, or security[13] Energy, water, buildings, and transportation are all part of a city's infrastructure. Many major cities own, operate, or regulate key public utilities that support the economy, health, and public safety of a city. The broad impact of these services, outdated systems, increased connectivity, and the wide use of third-party contractors all increase infrastructure vulnerability to extreme weather events and cyber attacks.

The US Department of Homeland Security said that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 198 cyber incidents reported by energy companies, public water districts, and other infrastructure facilities in the fiscal year ending September 30, 2012[14]. Recognizing the need to address such threats, the US National Institute of Standards and Technology (NIST) released a voluntary framework in February 2013, with an update in February 2014, to reduce cyber risks to critical infrastructure.[15] The NIST framework provides a flexible approach to determining controls and setting risked-based maturity models. It should be considered when developing a threat model and represents one way of structuring responses to infrastructure threats and general cybersecurity risks to city information systems.

9 Dynacare Laboratories, Notice of Privacy Incident, https://www.dynacaremilwaukee.com/Downloads/Dynacare%20SubNotice%20Rev112013.pdf

10 http://www.joburg.org.za/index.php?option=com_content&id=8771:22-08-2013-breach-of-our-it-system&Itemid=114

11 Softpedia, Hackers Attack "Heart" of US, District of Columbia site down, http://news.softpedia.com/news/Hackers-Attack-Heart-of-US-District-of-Columbia-Site-Down-265228.shtml

12 ZDNet, AFP and RBA websites hit by DDoS attacks, http://www.zdnet.com/au/afp-and-rba-websites-hit-by-ddos-attacks-7000023451/

13 Critical Infrastructure Protection Concepts and Continuum, http://www.microsoft.com/en-us/download/details.aspx?id=3251

14 Need citation

15 NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/

Learning from Estonia

In the spring of 2007, computer systems and networks in Estonia were subjected to a massive DDoS attack which emanated from abroad. Government services, such as the Ministry of Defense email network, in addition to private services, like bank websites and ATM networks, were disabled, rendering most public or private business effectively incapacitated during the roughly 48 hours of the attack. No physical damage occurred. Nevertheless, the attack intermittently paralyzed financial and government xctivity in the country for a period of a few weeks. The Estonian government and private sector used the incident to learn how to better protect their operations. Through public/private cooperation, Estonia has fortified electronic signatures, electronic failsafes, firewalls, and backup systems, and it has become a champion of cybersecurity.

The Cyber Attack on Saudi Aramco, Survival: Global Politics and Strategy April–May 2013.

Other factors to consider

In addition to the three areas addressed above, cities should consider a number of other factors when developing an understanding of the cybersecurity landscape. While not directly threats, these factors play an important role in a city's ability to respond.

Requirements and regulations

Understanding the threat landscape also requires knowledge of national or regional requirements regarding cybersecurity readiness. At this point, most national governments provide only voluntary guidance, but some are beginning to mandate compliance, in particular when it comes to critical infrastructures. In Japan, a new cybersecurity bill would require all government ministries and agencies to report cyber-attacks, giving the prime minister the authority to order them to comply.[16] Similar legislative requirements are being contemplated for critical infrastructure owners and operators in other parts of the world, such as in the European Union[17]. In some cases, some of these requirements could apply to city-owned and managed critical infrastructures. Cities should therefore watch these developments closely. In developing a threat model, cities should consider regulatory obligations and whether they need to update authorities or processes to improve cybersecurity risk management.

A city may also consider the need to develop procurement requirements or regulations to ensure that its cybersecurity needs are met, relative to the threats and risks it decides must be managed. If a city is considering these issues, it is essential that the city reflect on the balance of issues raised in this paper and look for technology-neutral and standards-based approaches to ensure technology service providers can meet a city's needs and the city can leverage the benefits of commercially available technologies in a cost efficient way.

16 The Japan Times, New cybersecurity bill would order all ministries to report attacks, http://www.japantimes.co.jp/news/2014/05/07/national/new-cybersecurity-bill-require-ministries-report-attacks/#.U4fDqqxOXbg

17 European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, July 2, 2013, http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=1666

Internal environment

After cities have evaluated their existing regulations and requirements, and determined whether there are gaps to address in terms of particular threats, they can assess their internal environment, beginning with:

- Enterprise architecture. Does the city have a current enterprise architecture to address system complexity and to determine how well systems align with city needs? If an enterprise architecture exists, is it being used across all agencies?
- Agencies. A clear map of all agencies and departments impacted by cybersecurity measures allows for easier communication and deployment. This should include determination of whether agencies and departments have written information security plans and policies in place and how often they exercise or test the plans.
- Audits. If security audits have been done, review past and current findings to better understand the efficiency and effectiveness of management, technical, and operational security controls needed to implement the information security plan.

Cybercrime costs the global economy up to 500 billion annually.

Funding

Money alone does not solve cybersecurity issues, which are ultimately a management challenge. City leaders need to make cybersecurity a priority and then look for operational efficiencies. It nevertheless needs to be recognized that funding will undoubtedly be required and, with pressing city priorities, it can be difficult to justify funding any preventive activities, which do not demonstrate an immediate impact. Some cities create champions, local government leaders who sponsor legislation and otherwise encourage funding. Education also plays an important role in convincing city funding authorities about the critical need for cybersecurity and how it can fit into the city's overall security approach. There may even be a national grant system for particular high-threat, high-density urban areas.[18]

Even without a large budget for cybersecurity, cities can create an overall information technology (IT) budget review process to ensure that old systems are retired and that new investments reduce administrative costs, create flexibility, and increase security. Many cities are turning to cloud computing to gain efficiencies in administration and operations and to improve security at the same time. Cities can also make smart security decisions in the procurement process, and look for ways to think about how to keep its top-tier security risks front of mind as it procures new products or services.

18 FEMA, Urban Areas Security Initiative, http://www.fema.gov/fy-2013-homeland-security-grant-program-hsgp-0

Steps to developing a cybersecurity strategy

This paper outlines six steps a city can take to develop a cybersecurity strategy. In order to help cities define the tasks within each step, there are specific recommendations and best practices included. These steps may be customized based on the needs of the city and will provide a framework for a workable and effective strategy.

1. Build a risk-based approach to cybersecurity
2. Establish clear priorities and security baselines
3. Coordinate threat and vulnerability information
4. Build incident response capabilities
5. Boost public awareness, education, and workforce training
6. Embrace public, private, and acedemic cooperation

1 Build a risk-based approach to cybersecurity

The first step in developing a cybersecurity strategy focuses on the risks to be identified, managed, mitigated, and accepted. There are a number of factors for city leaders to consider as they assess their risk landscape. Part of this work is threat modeling while other parts include setting up structures and procedures around risk.

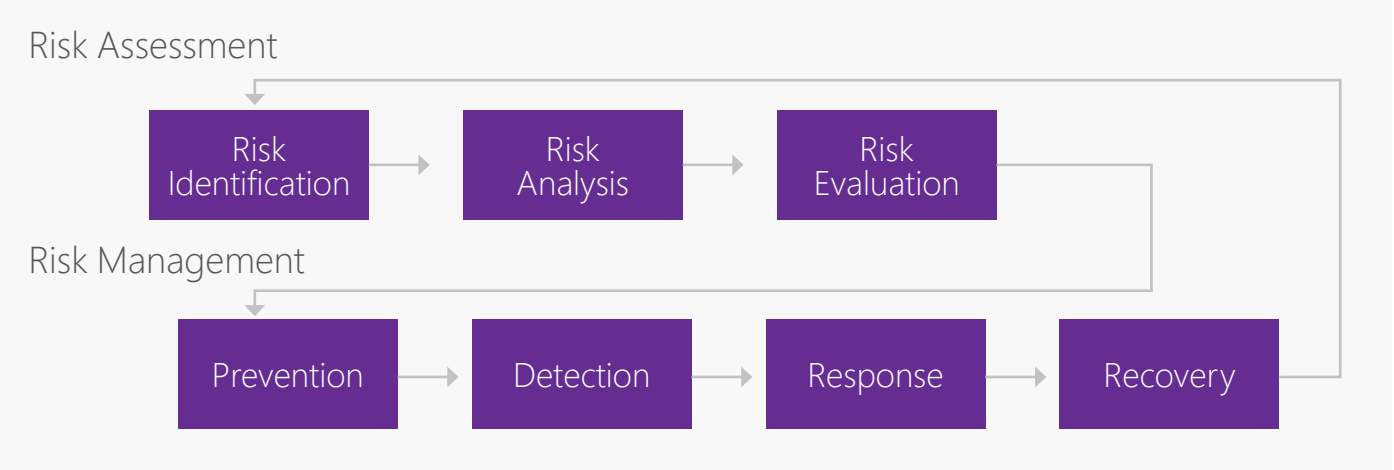
It may help city leaders prioritize this work if they understand the relationship between security and resiliency. In The Cybersecurity Risk Paradox, Microsoft finds a strong relationship between technology adoption and cyber incidents, particularly in emerging economies. The paper shows that countries that are above average in digital access, institutional stability, and economic development have correspondingly lower rates of malware.

A risk-based approach must look at the overall structure of a city's systems to determine where critical intersections occur and how to mitigate vulnerabilities to reduce the likelihood of system failure. City leaders should also consider leveraging table top exercises and technical reviews to understand interdependencies and single points of failure.

For most cities, balancing risk mitigation with other budget priorities will be an ongoing challenge but one that can be lessened by understanding the return on investment from cybersecurity measures. In 2014, the Center for Strategic and International Studies produced Net Losses: Estimating the Cost of Cybercrime; Economic Impact of Cybercrime II, which estimated that the likely annual cost to the global economy from cybercrime was $400 billion — or an estimated .8 percent of the global GDP. A city should consider the expense of cyber incidents on citizens, law enforcement, local businesses, and city administration to determine the return on investment for increasing cybersecurity measures.

Recommendations

- **Develop a clear structure for assessing and managing risk.** To simplify risk assessment and management, it is helpful to use the following taxonomy:



- **Determine the city's threat landscape through threat modeling.** A risk framework should include an understanding of threats and areas of vulnerability. When developing a threat model and prioritizing defensive efforts, a city can leverage information from other cities, private resources, and smart data. To simplify threat modeling, Microsoft has identified four major categories of cyber threats facing cities:

19 Microsoft, The Cybersecurity Risk Paradox, http://download.microsoft.com/download/E/1/8/E18A8FBB-7BA6-48BD-97D2-9CD32A71B434/Cybersecurity-Risk-Paradox.pdf

20 Net Losses: Estimating the Cost of Cybercrime; Economic impact of cybercrime II, 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Threat	Examples	
Passive	Unintentional actions	Exposure to malware through email or websites
		Receipt of spam email or phishing
	Under-resourcing	Unprotected systems
		Unclear mitigation strategies
		Undefined response capabilities
		Lack of clear ownership
Active	Cybercrime	Fraud
		Theft of intellectual property or finances
		Abuse or damage of ICT systems
		Damage to critical infrastructure
	Natural and manmade hazards	Typhoons
		Earthquakes
		Floods
		Tsunamis
		Accidental cutting of undersea Internet cables

These threats can have serious implications for data, systems, and infrastructure, including the theft of sensitive data, damage to business or operational systems, disruption of services, and other scenarios that could result in substantial financial loss and could compromise public safety. Each of these four areas should be included in the threat model for a city's strategy.

- **Document and review risk acceptance and exceptions.** When implementing a risk-based cybersecurity strategy, city leaders often find that some risks need to be accepted in order for the government to deliver services. It is impossible to mitigate all risk, and a framework for risk should include clear guidelines governing how risks are accepted and documented. These guidelines should also articulate when an asset is so vital that it should be protected at a higher standard. The risks being accepted and any relevant exceptions should be approved by the head of the responsible agency. In some instances, the risk should be taken to city leadership for acceptance.

  Within the cybersecurity strategy, city leaders should assign responsibility for accepted risks to pertinent personnel and should develop appropriate incident response plans to manage these risks in times of crisis. Registries of accepted risks should be reviewed on a regular basis to ensure that critical government-owned and private systems are not needlessly exposed.

- **Make citywide cyber risk assessment and management an ongoing process.** Risk assessment and risk management should be a continual process, not an end state. As technology evolves and threats grow more sophisticated, risk assessments and evaluations must assess whether current controls are still sufficient. Additionally, technologies may become available that allow for effective mitigation of previously accepted risks.

2 Establish clear priorities and security baselines

The threat model and risk assessment act as a foundation to help cities establish clear cybersecurity priorities and security baselines. Fortunately, cities can leverage existing standards to take the next step. The NIST Cybersecurity Framework consists of standards, guidelines, and practices which can be used by cities to manage cybersecurity-related risk.[21] Although it was published in the United States, the framework leverages work done around the world and makes sense for any city. Critical Security Controls, published by the Council on Cybersecurity, is another resource, providing recommendations for tangible methods to address risks to enterprise data and systems.[22]

One of the best ways to prioritize risks is to use existing standards, but risks often evolve too fast to be addressed by formal standards bodies. Additional risk management activities, such as a "top 20" approach, may augment standards to help prioritize risks.

Establishing a minimum security baseline for all systems and users, regardless of criticality, can also help prevent cybersecurity issues. A report published by Verizon[23] found that 97 percent of investigated network breach incidents in 2012 could have been prevented by using simple or intermediate security controls. Security baselines, based on pre-existing standards and tailored by agency and type of user, can help prevent such incidents and can better protect a city.

Recommendations

- **Set clear security priorities consistent with the strategy's principles.** Having a clear process to ensure that not all assets, systems, networks, or data are identified as high priority is critical to the successful implementation of the strategy. City leaders must review the strategy's principles and should align priorities accordingly. It is important to define and implement a clear framework for classifying systems and data as high, medium, or low impact and to then use this to evaluate key city systems—even those operated by third parties. In addition, to ensure a common approach across the city enterprise, cities should map protection profiles to the classification of systems and data.
- **Train city leaders to understand and support the principles and to manage priorities.** It can be difficult to weigh trade-offs when prioritizing cybersecurity—especially in a city with many disparate agencies. With regular training of city leaders about cybersecurity principles, it becomes easier to negotiate prioritization. Not all city leaders have a background in cybersecurity, but they can all be engaged in the prioritization process and can understand how decisions impact city assets.
- **Establish minimum security baselines.** By setting baselines, a city establishes a minimum standard for security of government data, systems, and infrastructure. But a baseline is just that—a starting place from which city leaders can continue to drive security enhancements. As cities regularly improve security procedures, baselines can be reevaluated. A strategy should include baseline parameters for:
  - **City systems**
    The city is responsible for establishing and meeting security baselines for all critical and non-critical government information and systems. To meet these security baselines, governments should hire or train cybersecurity and forensics experts to manage and defend networks. Governments should also establish and enforce procurement policies that result in the purchase of ICT products and services which are developed using a secure development process and which are then configured and deployed commensurate with risk.

21 NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/index.cfm

22 Council on Cybersecurity, Critical Security Controls Version 5.0, http://www.councilcybersecurity.org/practice-areas/technology

23 Verizon RISK Team, 2012 Data Breach Investigations Report. http://aka.ms/Verizon-Breach-Report-2012 , March 22, 2012.

- **All critical information and systems**
  Securing city information and systems is a mandatory starting place, but cities should also consider establishing baselines for all systems, regardless of whether they are under direct control. This may include mass transit, water, education, and healthcare—all systems with a broad impact for citizens. Using a standards-driven approach, such as recognizing products that have met the Common Criteria certification scheme or following other International Organization for Standardization (ISO) standards,[24] can assist cities in developing simple, more secure configurations that can be managed more easily by city ICT officials.
- **City suppliers and partners**
  Building a trusted supply chain is an important part of a city's cybersecurity efforts, and cities can act as both enforcers and educators in regard to suppliers and partners. By asking companies to adhere to specific security baselines or standards and by providing preference to companies that adhere to international standards, cities can help ensure that suppliers build in cybersecurity to product design and manufacturing.
- **Citizens**
  Cities should also encourage citizens to improve personal cybersecurity, since it reduces the likelihood of fraud and other criminal attacks and enables more confident consumption of e-government services. Providing tips for staying safe online, informing citizens of potential and real threats, and working with unique populations, such as students and local businesses, can help meet baseline requirements.

→ **Set clear roles and responsibilities.** Clear roles and responsibilities support the essential functions of a security baseline. If there is not a central agency responsible for ICT security, the cybersecurity strategy should recommend the establishment of an agency with appropriate skills, authority, and resources to develop an ICT security baseline and to implement the other requirements.

→ **Ensure resiliency for a city's network-based services.** A city's infrastructure is of little value if it is not consistently available. Resiliency may be met by migrating to a cloud-based service, or the network may require more bandwidth and capacity to ensure that a service remains operational during a crisis. A city's strategy should also consider the resources, standards, and organizational support needed to ensure that the most essential city services have a higher level of resiliency than less critical services, so that a city can prioritize its resources and efforts to ensure that its most essential services are always available.

→ **Recognize a role for continuous monitoring of systems and protection of data.** In a constantly changing threat environment, a city's cybersecurity strategy should recognize the need for continuously monitoring the security of systems, data, and infrastructure, rather than focusing on audits and paper-based compliance checks. Continuous monitoring uses automation to collect and analyze data from a variety of sources to maintain an accurate description of an organization's security posture to support organizational risk-management decisions.[25] Monitoring services should be divided into four categories:

- Baseline security monitoring for broad detection of malicious or anomalous network activity
- Specialized security monitoring for critical assets and critical processes
- Data analysis and reporting to provide telemetry to other key internal security detection and response partners
- Policy enforcement and measurement of control effectiveness

  There are standards, such as the NIST 800-53[26] standard , which include controls that address continuous monitoring. Using a broadly adopted standard to establish a citywide approach

24 U.S. Government Configuration Baseline (USGCB), http://usgcb.nist.gov/index.html

25 The U.S. National Institute of Standards and Technology (NIST) See, e.g., National Institute of Standards and Technology (NIST), "NIST Guide for Applying the Risk Management Framework to Information Systems (NIST Special Publication 800-37)"; ISO/IEC 31010:2009 - Risk management – Risk Assessment Techniques; and ISO/IEC 31000:2009 – Risk Management Techniques, defines continuous monitoring as "a risk management approach to Cybersecurity that maintains a picture of an organization's security posture, provides visibility into assets, leverages use of automated data feeds, monitors effectiveness of security controls, and enables prioritization of remedies." Available at http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf.

26 Need citation

for continuous monitoring of high-priority system and city websites. Furthermore, the use of appropriate analytics to understand and act on the data allows operators and auditors of government systems to be more responsive to changes in the threat landscape.

- **Establish technology-neutral software assurance and supply chain security policies.** When cities base their software assurance and supply chain policies on international standards, they create flexibility for suppliers and they increase the range of available solutions. Developing standards, such as ISO 27034[27] for secure software development and the better-known ISO 28000[28] for supply chain security, are useful references for establishing such policies.

  Supply chain security is complicated in a global economy. ICT components are manufactured and managed all over the world, and cloud computing, with data held in remote data centers, adds additional complexity. As described in the Microsoft white paper, *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*, a framework for managing supply chain concerns should rest upon four principles: a risk-based approach, transparency, flexibility, and reciprocity.[29]

  Core elements for reducing supply chain risk may include:

  - An overall threat model for supply chain risk, developed by the city and shared with its ICT vendors and suppliers.
  - Policies and controls to ensure that the government is buying genuine products from trusted sources, in addition to capabilities that can identify and remove counterfeit or gray-market products that can create risks to the integrity of government information, services, and assets.
  - A lifecycle approach to government systems that extends beyond the procurement phase and addresses the controls needed to ensure that the process for updating systems and retiring systems does not introduce risk into organizations.
  - Mechanisms to ensure that suppliers have demonstrable processes for: managing employee identity, including tying identity to role-based access for system development and production; a secure development process, such as the Microsoft Security Development Lifecycle (SDL) and ISO 27034-1; code integrity practices that prevent or remediate potential risks associated with intentional or unintentional insertion of malware; digitally signing code; and swift recognition of counterfeit products.

- **Run up-to-date software, and migrate off of unsupported software.** One of the best defenses against cyber threats is to operate patched and up-to-date software. Unsupported software does not benefit from patches that can head off security issues before they occur. According to the Federation of Small Businesses and the Home Office and Business Departments in the United Kingdom, small- and medium-sized businesses lose more than £785 million per year to cybercrime.[30] According to the report, "Only 36% of businesses are regularly installing vendors' security patches." Systems running on Windows XP are now particularly vulnerable because attackers are known to reverse-engineer released patches to uncover potential vulnerabilities in older systems. Vulnerabilities or weaknesses that can be exploited *will* be exploited.

  The necessity for systems to be up-to-date and fully patched cannot be understated. A city's strategy can include tracking systems as they reach their end of life and products or services as they reach their end of support, so that security issues are managed and risks are not left until it is too late.

- **Leverage procurement processes to reflect priorities and risks.** Cities have the ability to take the principles and priorities deduced through risk identification and ensure that those issues are reflected in a city's IT procurement or regulatory approaches. Cities can use the procurement process to learn about new technologies or capabilities that may help increase a city's security baseline, and help refine the way in which the city thinks about its technology lifecycle.

27 Need citation

28 Need citation

29 Microsoft, Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust, http://www.microsoft.com/downloads/en/details.aspx?FamilyID=cb3cf551-c1e5-4be6-bf54-27d9cf852910

30 Small firms lose up to £800 million to cyber crime, says FSB, Federation of Small Businesses, http://www.fsb.org.uk/News.aspx?loc=pressroom&rec=8083

3 Coordinate threat and vulnerability information

Sharing information quickly with specific mitigation guidance or updates to remediate vulnerabilities is key to defeating cyber threats. Working hand in hand with the private sector and other government entities to identify vulnerabilities is just part of the picture. There must be actionable steps that city agencies and citizens can take after vulnerabilities are exposed. In the case of threats, information needs to be shared as quickly as possible to the widest audience so that threat actors can be stopped with minimal damage. A city's system should consider threats and vulnerabilities to data and to infrastructure and should determine criteria for when and how information is shared. A recent discovery of the Heartbleed vulnerability in OpenSSL raised questions of whether information was shared soon enough to prevent harm. It also brought up the subject of how best to ensure that mitigations are developed and shared broadly to better protect the computing ecosystem.

Recommendations

- **Set expectations for sharing threat and vulnerability information.** Everyone benefits when cities partner with national entities and the private sector to quickly share information about new threats and vulnerabilities. A city's cybersecurity strategy should recommend a clear communication path between city, regional, and federal government, along with the private sector.
- **Create a cross-city mechanism for sharing.** A city's strategy should include recommendations for sharing information about incidents and indicators for compromise. Cities should share this threat information within its agencies to better manage risk and to encourage cooperation and learning among city ICT professionals. Additionally, cities may want to share information with critical industry and infrastructure owners and with companies that have the ability to develop and disseminate updates to their customers. Having the right legal and technical frameworks in place to enable sharing will help ensure a more effective response process and help parties stay more focused on essential threats. This open sharing of information promotes stronger partnerships with the private sector and helps ensure that everyone is focused on critical threats.
- **Create a Computer Emergency Response Team (CERT).** CERTs are not limited to national entities. Government organizations, private companies, and universities all develop CERTs to coordinate threats and vulnerabilities. The Forum of Incident Response and Security Teams (FIRST) coordinates more than 300 member teams across 66 countries for cooperation and coordination in incident prevention, rapid reaction to incidents, and information-sharing.[31] This resource can act as a starting place for cities interested in creating a CERT.

  A city's strategy should include a requirement to draw vulnerability and mitigation information from trusted sources, such as national CERTs. A national CERTs acts as a hub for alerts and giving cities prescriptive guidance on sharing that information with citizens. Additionally, cities can create ongoing partnerships with the private sector, particularly technology companies, which may have dedicated resources to research and identify cybersecurity concerns.
- **Apply relevant national or international standards for information-sharing.** Relevant standards can bolster readiness in government agencies and in private enterprises. Encouraging more common approaches to vulnerability management and information-sharing should be incorporated into a city's cybersecurity strategy. For example, the strategy can encourage those responsible for information-sharing and threat and vulnerability assessment to reflect the ISO/ International Electrotechnical Commission (IEC) standards on vulnerability handling

FIRST

The Forum of Incident Response and Security Teams is an international organization of computer incident response teams from the public and private sector which cooperatively handle computer security incidents and which promote incident prevention programs.

Membership in FIRST enables response teams to more effectively handle security incidents by providing access to best practices, tools, and trusted communication with member teams from around the world.

31 FIRST, http://www.first.org/

within an enterprise (ISO/IEC 30111)[32] and vulnerability disclosure external to an enterprise (ISO/IEC 29147).[33] These standards greatly improve the ability to handle complicated issues related to response. Also, encouraging greater use of Common Vulnerabilities and Exposures (CVE)[34] identifiers, and taking steps to assess the severity and exploitability of a vulnerability, can increase capacity and readiness for complex response events. There are also machine-to-machine information-sharing standards, such as the Structured Threat Information eXpression (STIX)[35] and the Trusted Automated eXchange of Indicator Information (TAXII)[36] to represent structured cyber threat information.

- **Run drills for cyber threats. Drills, with real scenarios and participants, are important for cities to test their game plans.** Such drills should include personnel from across multiple city, state, and federal agencies, along with participants from the private sector—all members of a city's cyber incident response team. Conversely, cities can provide resources to help local businesses run their own cyber drills, such as those run by the City of San Diego and the Naval Postgraduate School, which support local companies.[37]
- **Emphasize privacy and civil liberty protections in threat information-sharing.** There is much discussion about the appropriate level of information that can and should be shared between private sector entities looking to respond to vulnerabilities or threats, and between those private sector entities and government agencies. It is important that a cybersecurity strategy emphasize the steps to be taken to ensure that privacy risks are mitigated across the data lifecycle. Ensuring adequate judicial oversight and enforcement of privacy protections becomes increasingly important in connected societies. Threat and vulnerability information-sharing procedures should also reflect existing privacy laws in the city and the country—and even internationally—as information is shared across borders.

32 ISO/IEC 30111:2013, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53231

33 ISO/IEC 29147"2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

34 CVE International, http://cve.mitre.org/

35 Structured Threat Information eXpression, http://stix.mitre.org/

36 Trusted Automated eXchange of Indicator Information, http://taxii.mitre.org/

37 Forbes, Channel Your Inner Hacker and Other Cyber Security Suggestions, October 11, 2013, http://www.forbes.com/sites/xerox/2013/10/11/channel-your-inner-hacker-and-other-cyber-security-suggestions/

4 Build incident response capabilities

Cyber threat response requires sufficient capabilities to protect a city's people, information, systems, and infrastructure. A city's cybersecurity strategy should include a definition of which threats fall under the city's purview and which belong to the private sector, with a communication plan that bridges the two. As indicated earlier, threats should be prioritized and a hierarchy of threats and associated responses, structured based on the anticipated impact, should be developed. It is important for cities to recognize that a threat to critical infrastructure systems, such as water or power, requires a significantly different response than a threat to an isolated set of data or systems.

Integrating cyber incident response into a city's existing incident command structure is another critical element of the strategy. In most cities, law enforcement and emergency services can provide established resources and personnel for cyber response. A city's police department may include a cyber-forensics department or staff that can be incorporated into the city's cyber response command structure, empowering them to identify, triage, and thwart cyber threats. An example of how one city has dealt with this issue, is the Los Angeles Cyber Intrusion Command Center, operated by the Los Angeles Police Department, with members from city and federal agencies. The 24-hour operations center monitors cyber-threats against the city, and members meet regularly to discuss common threats and possible methods of neutralizing them.

Fusion Centers, information-sharing centers originally developed in the early 2000s under the U.S. Department of Homeland Security, can provide a model for integration of existing incident response capabilities into cybersecurity. These centers empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to lawfully gather and share threat-related information.

Recommendations

- **Set clear definitions and procedures for incident response.** A cybersecurity strategy must clearly define what constitutes a cyber-incident that requires government involvement and that triggers incident response plans and procedures. These cyber incidents will likely, and reasonably, focus on disruptive, exploitative, or destructive attacks against a city's citizens, information, systems, or infrastructure.[40]
- **Create clear ownership.** A cybersecurity strategy should recommend that the CERT lead coordination between public and private sectors responding to cyber incidents. The strategy should task the CERT with the technical and managerial capabilities to effectively assist government and critical private actors during crisis situations.
- **Enable consistent incident classification.** When defining incident response, cities should clearly distinguish between incidents requiring a city's response and those which do not rise to that level. A city's role, whether in providing direct defense or indirect support, may vary based on the relationship between private critical infrastructure and the government.
- **Engage private sector and national resources.** City agencies should work with the private sector to respond to cyber incidents. This includes clear communication paths about threats and vulnerabilities, along with sharing resources and training. For example, the City of London Police developed a program with the British Bankers Association to train bankers to identify and respond to cybercrime. The program plans to provide workshops for banks around the world on threat identification and mitigation.

40 City of London Police, Fraud experts to train thousands of bankers to create 'virtual ring of steel' in City to combat fraud and cybercrime, http://www.cityoflondon.police.uk/news-and-appeals/Pages/fraud-experts-to-train-bankers.aspx

- **Test incident response capabilities and processes.** Just as city systems are tested for major catastrophes, such as earthquakes, hurricanes, and terrorist activity, cyber response capabilities should be routinely analyzed against the current threat landscape. When integrated into existing response procedures run by fire and police departments, these response efforts become more effective and are better managed and scaled. A cybersecurity strategy should include specific expectations for the private sector and for other government entities. Exercises, involving both government and private sector actors, help stakeholders understand their roles during a crisis and can better prepare them for incident response scenarios.
- **Consider privacy needs in all parts of incident response.** Just like all law enforcement efforts, cyber incident response must protect the privacy and legal rights of citizens. A cybersecurity strategy should recommend that all responders receive training in information privacy and on relevant national and local laws and reflect a legal structure that facilitates information sharing while neutralizing any private data or unintended data. Specific principles, such as limiting the use and sharing of data, should be a part of an incident response plan to help ensure citizens' civil liberties.

5 Boost public awareness, education, and workforce training

A vast number of cyber incidents are caused unintentionally by actions of employees or citizens. Just one person needs to click an infected link or email to put an entire network of systems and information at risk. One such virus attack downed a turbine control system at a US power company for three weeks, when a technician unknowingly inserted an infected USB drive into the network.[41] Cities play an important role in equipping employees and citizens with tools and resources to be cyber smart. Preventive education not only protects data, systems, and infrastructure but also saves money in cybercrime enforcement and cleanup. Public awareness efforts can include cyber smart campaigns, such as the one run by the City of Boston.[42] The campaigns include education about browser safety and device security measures, along with advice on when and where it is safe to share personal information online. As early as 1999, the European Commission ran the Safer Internet Programme, which led to Safer Internet Day,[43] a program that highlights the importance of online safety and security. It has grown into a 100-country effort supported by the Insafe Network.[44]

Workforce training for city and private sector employees is also an important part of a cybersecurity strategy. A city's strategy can provide recommendations for cyber training programs at the university level, along with executive and employee training for private sector companies.

Finally, cities may also choose to require citizens to perform device checks before accessing city systems, reinforcing smart cyber behavior. It is crucial that a city's cybersecurity strategy recognize that citizens should receive training to practice smart and safe computing.

Recommendations

- **Develop public awareness and education campaigns.** A city's strategy should assign an agency or entity responsibility for raising public awareness of risks and the need for cybersecurity. National and regional cybersecurity months or days are good ways to provide educational information for citizens. An educational campaign should reflect the needs of unique groups, including:
  - **Students.** School districts can play an important role in educating young people about online security and smart online behavior. StaySafeOnline.org provides lesson plans, activities, and exercises for all grade levels. The organization breaks down cyber safety into simple steps, including: keep a clean machine, protect your personal information, connect with care, be web wise, and be a good online citizen.
  - **Universities.** Academic institutions are major targets for cyber-attacks because of the intellectual property they hold within their systems. A dramatic increase in breaches has forced universities to rethink their security structures and policies.[45] Cities can work with local universities to educate students and employees on the threats facing university data, plus measures to keep information secure.

SIMPLE STEPS FOR COMPUTER PROTECTION

- **Install antivirus software, and regularly update it.**
- **Install hardware/ software, such as a firewall, to manage communication between and among networks.**
- **Have an offsite backup of important files.**
- **Require the user to authenticate when signing in.**
- **Regularly install operating system patches.**

41 MSN News, Homeland Security says criminal virus shuttered power plant, http://news.msn.com/science-technology/homeland-security-says-criminal-virus-shuttered-power-plant

42 City of Boston, Cyber Security, http://www.cityofboston.gov/oem/ReadyBoston/cybersecurity.asp

43 Safer Internet Day, http://www.saferinternetday.org/web/guest/about

44 Insafe Network, http://www.saferinternet.org/

45 International New York Times, Universities Face a Rising Barrage of Cyberattacks, http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html

- **Seniors.** Older people may be more vulnerable to both targeted and broad-based online threats because of a slower rate of Internet adoption. Pop-up browser windows may trick seniors into downloading infected software, and email phishing scams may entice older citizens to give away personal and financial information to criminals. Cities can work with organizations targeted to seniors on ways to stay safe in cyberspace. One private-public partnership is the Microsoft and Miami program called eSeniors, providing free computer training and reduced-price technology packages to Miami seniors at learning hubs in neighborhood senior centers.

➔ **Cultivate employee development and workforce training programs.** Cities often struggle to attract and retain a talented workforce commensurate with private enterprise. Incentives, such as reduced college tuition and additional training, can help bridge this gap. A cybersecurity strategy should include plans to ensure a pipeline of well-trained city technologists for future IT leadership roles. In the United Kingdom, the government announced plans to increase education for cybersecurity professions, including apprenticeships for older students. Another program, the Cyber Security Challenge UK, connects public and private sector organizations to bring talented people into the field of cybersecurity.

6 Structure public, private, and academic cooperation

It wasn't long ago that data and systems security was managed solely by a chief information or technology officer. However, experts point out that "With the litany of high-profile cybersecurity hacks, and the potential resulting drop in shareholder value, regulatory inquiries and litigations which inevitably follow, cybersecurity has become an increasingly challenging risk that boards must address."[48]

Today, leaders in all departments of both private and public organizations are concerned about cybersecurity. This is good news for cities. Not only are national, state, and regional governments prioritizing the issue, the private sector is investing heavily in related systems and personnel. Collaborating with the private sector, other public sector entities, and academic institutions to research, identify, and respond to cyber threats must be a critical component of a city's cybersecurity strategy.

In much of the world, critical infrastructure is managed by government-controlled private entities, making cooperation even more important. A city's cybersecurity strategy can formalize the creation of Public Private Partnerships (PPPs) to benefit everyone. The European Union Agency for Network and Information Security published the *Good Practice Guide on Cooperative Models for Effective Public Private Partnerships (PPPs)*,[49] which offers 36 recommendations on how to build successful PPPs for resilient security. This is an excellent starting place for cities looking to formalize partnerships.

Cooperation should also be developed amongst city agencies. At the simplest level, this means recommending ways for city agencies to internally communicate and collaborate on threat information, best practices, and incident response. From there, cities should recommend ways to partner with other cities and regional governments, without regard to national boundaries. Cybersecurity allows cities to consider new models of engagement in which information, resources, and expertise are shared openly to combat common dangers.

Cities can look at the work of C40 as a model for organic city-to-city collaboration. In 2005, megacities came together to reduce carbon emissions and to increase energy efficiency around the world. Led by mayors and city leaders, C40 works closely with participating cities to address climate risks and impacts on a local and global level.[50] And they are making a difference. According to C40 Chair, Rio de Janeiro Mayor Eduardo Paes, "Mayors have real power to cut emissions and improve climate resilience and they are taking action. C40's networks and efforts on measurement and reporting are accelerating city-led action at a transformative scale around the world."[51]

Recommendations

- **Utilize private sector resources.** Local companies generally participate in civic life with programs that range from loaned executives to specialized training. A cybersecurity strategy should recommend the creation of programs that tap private sector companies. A loaned executive program, where private sector employees act as unpaid city employees, can fill specific cybersecurity needs within a city's ICT organization and can provide expertise and new perspectives. Cities can also work with companies to inspire innovation among employees and citizens. For example, Microsoft has more than 100 state-of-the-art Innovation Centers

48 International Association of Privacy Professionals, The Privacy Advisor, Cybersecurity in the Boardroom: The New Reality for Directors, https://www.privacyassociation.org/publications/cybersecurity_in_the_boardroom_the_new_reality_for_directors

49 European Union Agency for Network and Information Security, Good Practice Guide on Cooperative Models for Effective PPPs, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

50 C40, www.c40.org

51 C40Cities, Infographic: C40 Cities Releases Landmark Research Revealing Expansion and Acceleration of Climate Actions in Megacities, http://www.c40.org/blog_posts/infographic-c40-cities-releases-landmark-research-revealing-expansion-acceleration-of-climate-actions-in-megacities

around the world, offering organizations access to valuable resources, experts, and tools for collaboration and skills development.

- **Partner with universities.** Cities can support cybersecurity research and training at local universities and subsequently benefit from the outcomes. Increasing the number of trained cybersecurity professionals within a region can help a city recruit and employ top-notch experts. Universities can also provide valuable research into threats and vulnerabilities within a city.
- **Address procurement and grant-making.** A city's cybersecurity strategy can define guidelines for ICT procurement that reflect a city's cybersecurity priorities and a city's technology lifecycle, as well as leverage federal certifications and evaluations rather than replicating those efforts. As service providers continue to look for new products and services for their customers and as security plays a larger role in procurement, it will likely drive innovation in the marketplace.
- **Sponsor events to connect public and private sector.** Events can range from large annual summits of international representatives to smaller, more regular meetings with startups to boost innovative thinking.
- **Promote law enforcement cooperation while protecting privacy and civil liberties.** These are uncharted waters, and law enforcement agencies must navigate ways to work with responders around the world, despite different values around privacy and different technology capabilities. A cybersecurity strategy should recommend that a single entity, likely within the existing police department, take responsibility for cybersecurity issues and that adequate training and resources are provided to this entity with appropriate laws and oversight to ensure privacy and civil liberties are protected and respected.
- **Create a culture of ICT innovation.** An innovation culture propels organizations that thrive in the new economy. Cities can create environments that encourage innovation. Tech City UK is developing tech clusters to help digital businesses grow and develop new ideas. They provide advice on everything from staff recruitment, accounts preparation, and compliance to negotiating leases, marketing, and raising investment. Other services include tax breaks, community events, and technology competitions. In February 2014, during the worst flooding seen in recorded UK history, various government agencies opened up government flood-level data for a day-long #floodhack, hosted by Tech City UK, allowing developers to create innovative solutions to the weather-related disasters. Seven applications were shortlisted for further consideration. [52]

52 Tech City UK, Tech City UK Convenes Developer Talent and Tech Community to Host #floodhack in Shoreditch, http://www.techcityuk.com/press

Conclusion

This is just the beginning of an age of sophisticated technology that will broaden the possibilities for humankind, while exposing people to unimagined dangers. Connected devices, intelligent buildings, and smart grids signify the beginning of the tectonic shift in human experience that compares to the discoveries of early seafaring explorers. Like these discoverers, there are few laws or prevailing norms to chart the course into cyberspace, and cities play an important role in shaping this future.

Establishing a city strategy for cybersecurity is an important element in maintaining a city's security while mapping a path for future resilience. By creating a principled approach, thinking holistically about threats and vulnerabilities, and deploying strong practices to detect, mitigate, and communicate threats, a city can protect its citizens and safeguard its resources. Nevertheless, there will be barriers in the way. Strained city budgets can limit planning and development. Risk-averse city managers may inhibit collaboration and innovation. Privacy concerns may restrain activities. By clearly articulating the return on investment—financial, security, and quality of life—a cybersecurity strategy can overcome these obstacles and become an integral part of a city's transformation.

Microsoft supports city efforts to develop cybersecurity strategies. With much of the world's population located in urban areas, cities are uniquely positioned to confront and manage cybersecurity concerns. Microsoft stands ready to help city leaders keep their communities, and the world, safe and protected.

Cybersecurity strategy checklist

1. Build a risk-based approach to cybersecurity

- ☐ Develop a clear structure for assessing and managing risk.
- ☐ Determine the city's threat landscape through threat modeling.
- ☐ Document and review risk acceptance and exceptions.
- ☐ Make citywide cyber risk assessment and management an ongoing process.

2. Establish clear priorities and security baselines

- ☐ Set clear security priorities consistent with the strategy's principles.
- ☐ Train city leaders to understand and support the principles and to manage priorities.
- ☐ Establish minimum security baselines.
- ☐ Set clear roles and responsibilities.
- ☐ Ensure resiliency for a city's network-based services.
- ☐ Recognize a role for continuous monitoring of systems and protection of data.
- ☐ Establish technology-neutral software assurance and supply chain security policies.
- ☐ Run up-to-date software and migrate off of unsupported software.
- ☐ Create procurement processes to reflect priorities and risks.

3. Coordinate threat and vulnerability information

- ☐ Set expectations for sharing threat and vulnerability information.
- ☐ Create a cross-city mechanism for threat and vulnerability information sharing.
- ☐ Create a Computer Emergency Response Team (CERT).
- ☐ Apply relevant national or international standards for information-sharing.
- ☐ Run drills for cyber threats.
- ☐ Emphasize privacy and civil liberty protections in threat information-sharing.

4. Build icident response capabilities

- ☐ Set clear definitions and procedures for incident response.
- ☐ Create clear ownership.
- ☐ Enable consistent incident classification.
- ☐ Engage private sector and national resources.
- ☐ Test incident response capabilities and processes.
- ☐ Consider privacy needs in all parts of incident response.

5. Boost public awareness, education, and workforce training

- ☐ Develop public awareness and education campaigns.
- ☐ Cultivate employee development and training programs.

6. Structure public, private, and academic cooperation

- ☐ Utilize private sector resources.
- ☐ Partner with universities.
- ☐ Address procurement and grant-making.
- ☐ Sponsor events to connect public and private sector.
- ☐ Promote law enforcement cooperation while protecting privacy and civil liberties.
- ☐ Create a culture of ICT innovation.