

Introduction ▶

Smart technology for managing public infrastructure: Three key areas of use ▶

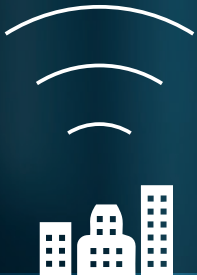
Three risk categories public entities should understand ▶

Actions to consider for minimizing risk ▶

Insurance considerations ▶

How Travelers can help ▶

Infrastructure for the smart city



How does a smart city prepare for infrastructure risks?

Management of infrastructure ranks among the most important responsibilities that public entities face. Effective maintenance of water and sewer systems, power grids and buildings can contribute significantly to a local community’s way of life. Ineffective or inefficient management can spell disaster.

Cities and other public entities increasingly look to certain types of smart technology to enhance their ability to manage public infrastructure, often to gain efficiency or reduce costs. New Internet of Things (IoT) devices act as key enablers to these capabilities, as sensors capture and relay information on water usage, energy consumption and building environmental conditions. Taking such metrics as inputs, powerful software enables better insights and more effective action. As more public entities achieve success by applying smart technology to infrastructure, others are beginning to evaluate their options.

Public entities face risks whenever they deploy a new technology in service of their infrastructure. This includes new opportunities for cyber breaches, property damage and bodily injury. Any public entity considering such systems should understand and prepare for the inherent risks.

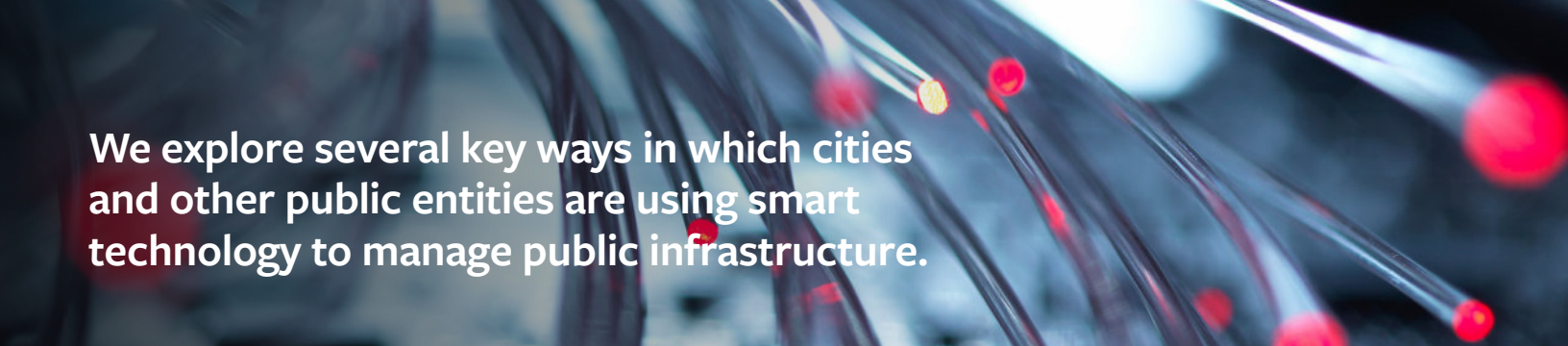
– *Melanie Wahlquist*
Chief Underwriting Officer, Public Sector Services at Travelers

IMPORTANT NOTE

The “illustrative risk scenarios” described in this document are intended to facilitate consideration and evaluation of risks, and are not necessarily based on actual events. In addition, these risk scenarios are not a representation that coverage exists or does not exist for any particular claim or loss under any insurance policy or bond sold by Travelers or other carriers. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions and any applicable law. Some risks may not be insurable. Companies should consult an independent agent or broker to evaluate what coverage is right for them.

The “actions to consider for minimizing risk” described in this document are also intended to facilitate consideration and evaluation of how risks can be mitigated. These are not direct guidance or advice on what actions should be taken. Other actions may be appropriate, depending on the circumstances. Companies should consult an independent agent or broker to evaluate what risk management products or services are right for them.

The reference to any information regarding any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply a Travelers endorsement, recommendation or favoring of such item or organization. Any such reference is for informational purposes only. Any potential user of any product identified is expected to conduct their own due diligence and assessment of the vendor, product or services as appropriate for their needs.



We explore several key ways in which cities and other public entities are using smart technology to manage public infrastructure.

Introduction

Over two decades ago, cities started investing in microsensor applications. However, few envisioned a day when they would rely on connected computer systems to control mission-critical municipal services like traffic control, energy optimization and secure building access. Most city managers took a cautious wait-and-see approach, allowing the early adopters to either prove or disprove the new technology's promises.

Today, however, there are fewer factors holding them back. Ongoing migration to cities places strain on infrastructure, requiring greater efficiencies. Increased citizen expectations for “connectivity” calls for integrating technology to enable more transparency. High-profile success cases give many confidence that they can also find success with the technology.

Definitions for “smart technology” vary among those who use the term for either technical or marketing purposes. For the purposes of this

document, however, we are defining public infrastructure “smart technology” to include connected devices or software intended to enhance or automate tasks performed by public entities for the management of public infrastructure. The Internet of Things (IoT) is a concept that relates closely, as many smart devices are internet-connected or analyze data from internet-connected devices.

On the pages that follow, we explore several key ways in which cities and other public entities are using smart technology to manage public infrastructure. Then, we identify and explore key risk categories impacting the cities that deploy this technology and highlight several specific actions to consider to minimize risk. Finally, we conclude by sharing insurance considerations that public entities should discuss with their independent agent or broker.

Smart technology for managing public infrastructure: Three key areas of use

The benefits of smart technology are far reaching, impacting every aspect of city life. However, there are three key areas of use where small and large cities are focusing their attention. In these three areas, cities have found solutions that work and are making a major difference in their economy, their way of life and their ability to serve residents.



1. SMART WATER AND SEWER SYSTEMS

In the U.S., supplies of clean running water have been running consistently for so long that we can scarcely imagine a day when there might not be enough for everyone. However, a study by the United Nations' 2030 Water Resources Group shows that if current consumption trends continue, the demand for water will exceed supply by 40% by the year 2030.¹ Because the problem doesn't generate much press coverage, few private companies have devoted R&D resources to address it, leaving municipal governments to seek other solutions.

Sensors can help city water managers in several ways. By embedding water sensors inside of reservoirs, dams and pipelines, city officials can chart water supplies to determine exactly when and by how much water supplies are increasing. Likewise, they can monitor how much water is being delivered to residential areas and workplaces. Embedded sensors can detect pipeline leaks and blockages, and also pinpoint where the most water is being lost. Managers then know where to send work crews for repairs to keep the water flowing steadily through the supply chain. With accurate real-use figures, cities can better develop water usage plans and understand shortages their municipality may face.

Water supply is also an aspect of private home ownership that is becoming a public concern. Homes may have leaking pipes and valves that homeowners aren't even aware of. The cost of these leaks can amount to hundreds and, sometimes, thousands of dollars per year in wasted water. As water supplies tighten in some parts of the country, finding these leaks and fixing them becomes an integral

part of a city's ability to conserve its water supply. Smart technology can play a role in solving this problem, with connected sensors that detect pipe ruptures and automatically shut off the water flow until repair crews can fix the problem. The sensors send an internet alert to property owners so that they're informed of the issue.

Most consumers are happy to conserve water, but don't know where to start. The city of East Bay, California, has teamed up with WaterSmart, a software vendor, to address this problem by giving customers access to a web portal that compares the water consumption of other homes of comparable size within the city. This helps consumers understand how and when they're using the most water, and even gives them tips on how to consume less when using showers, appliances and swimming pools.

As many public entities face aging infrastructures, more are faced with leaks occurring in underground pipes. Often called "ghost water," this water is the difference between the volume of water produced and the volume that is billed for. For one city in Kansas, this leaking water added up to billions of gallons lost, and even worse, millions to ratepayers' bills. While the value of the water lost is very concerning, the leaky systems can cause even bigger problems, including flooding, expensive repairs and contaminated drinking water.² Sensor-generated water data not only aids in the conservation effort, but can also be used as input for city planning. When water companies and civic leaders work together, the net result is more effective planning, better service delivery, increased savings and more available capital to invest in additional urban innovation.



2. SMART ELECTRICITY AND POWER GRIDS

The modern power grid is a true engineering marvel. In the U.S., more than 9,200 power generating stations send over 1 million megawatts across 300,000 miles of transmission lines. However, most American city power grids in use today were originally designed in the late 19th century and gradually improved upon as technological advancements became available. Because the grid's foundation was designed in an era of antiquated technology, the entire system suffers from inefficiency and rapidly increasing transmission and generation costs.³

The Hawaiian island of Maui is modernizing its power service with new smart grid technology it calls the "Internet of Energy." Advanced computer systems monitor power lines to better manage electricity delivery. Smart meters carry two-way (machine-to-machine) communication between the power company and individual homes over a secure wireless network, improving overall system reliability. Power line sensors automatically notify the utility of an outage in real time, while a revolutionary battery energy storage system stores excess energy to be used later at high-demand levels. The Maui Smart Grid increases local renewable energy supplies while improving overall system reliability.⁴

In addition to saving cities transmission and generation costs, sensor-based systems also help customers manage their own power consumption. Idaho Falls Power (IFP) in Idaho Falls, Idaho, began installing its first state-of-the-art electric meters at customer homes and businesses in 2012. Today, IFP has over 27,000 smart meters that transmit usage data over a wireless network complete with alarms to detect sensor tampering. The utility also provides a free web portal that lets consumers drill down by the hour into their power usage throughout the billing cycle. With more visibility into voltage levels, both IFP and its ratepayers share significant utility cost savings.⁵

By renovating aging power grids, public entities can achieve greater electricity throughput, enhance efficiency and lower transmission costs.

Stray voltage refers to the loss of electrical power due to the difference in capacity between two locations joined by power lines. Not only is it costly in terms of lost electric power, but it can also electrify nearby objects with enough voltage to be dangerous to both humans and livestock. Two Con Edison researchers have come up with a cost-effective way to detect and report stray voltage using the sensors built into smartphones and tablets. Utility workers' phones sense the presence of stray voltage, then send the captured data to Con Edison via wireless data transmission components that come standard on most smartphones – no additional hardware required. "The smartphone electric field readers can interpret the harmonic content of energized objects," says Paul Richardson, one of the inventors of the new system. "This information can help us determine the source of the voltage condition and its potential to manifest itself into real line voltage."⁶

By renovating aging power grids, public entities can achieve greater electricity throughput, enhance efficiency and lower transmission costs. Power companies can smooth out the peaks and valleys of power demand with new digital delivery methods and machine-to-machine communications while providing a safer, more reliable electric utility service to the citizens and businesses they serve.



3. SMART PUBLIC BUILDINGS

Market research company International Data Corporation (IDC) defines a smart building as “a facility that utilizes advanced automation and integration to measure, monitor, control, and optimize operations and maintenance.”⁷ The technologies that enable all of these functions rely heavily on sensory input, big data management and advanced analytics to keep the buildings operating efficiently. A back-end building automation system accepts the sensory input to optimize building functions like temperature regulation, humidity control, system maintenance and admission to private areas. In essence, the smart building acts both as the producer and consumer of its own data to enhance the facility’s operational purpose and extend its useful life.

Energy savings alone will likely pay for the cost of the sensor integration. According to the Environmental Protection Agency (EPA), the average commercial building loses 30% of its energy, resulting in \$60 billion of aggregate waste per year. Those same buildings can expect to save anywhere between 10% and 25% on HVAC alone by integrating sensor technology – a potential savings of \$15,000 to \$50,000 per building per year with no additional human input required.

Buildings enabled with smart technology relieve human managers from the time-consuming task of gathering data and adjusting maintenance controls manually. This, in turn, allows property managers to control far more buildings than their typical span of control will allow. This benefit can’t come soon enough; as people continue to flock toward cities, the demand for more smart buildings will continue to rise.

Smart sensors can also guard access to sensitive locations within buildings themselves. In areas that demand high security, such as courthouses and jails, facial recognition sensors can detect a person’s identity and lock or unlock passageways accordingly. By cataloging the facial features of known terrorists and criminals, law enforcement agencies can detect and remove high-risk individuals before they have a chance to commit crimes or acts of terrorism (see Travelers Risk Advisor Series Issue, “Public Safety for the Smart City”).

The smart building acts both as the producer and consumer of its own data to enhance the facility’s operational purpose and extend its useful life.



CYBER



**PROPERTY AND
COLLATERAL DAMAGE**



BODILY INJURY

Three risk categories public entities should understand

Smart technology holds the potential to impact infrastructure across America, bringing unprecedented levels of convenience and productivity. However, it's important to realize that very few elements of public infrastructure were designed with machine-to-machine communication in mind; every sensor advancement requires technological retrofitting, which comes with its own set of inherent problems. And because smart city technology is so new, no one is completely certain of the risks involved should a device malfunction or fall victim to a malicious cyber attack.

Cyber

Cyber risk continues to be a major concern for public entities, regardless of size or geographic location. Many things could trigger a cyber breach; a viral attack, ineffective IT security or a security software failure could create an opening for a breach, bringing disastrous financial and political results. The 2016 Ponemon Institute cyber crime study shows that, in 2016 alone, there were 47,237 cybersecurity incidents and 193 breaches with confirmed data loss in the public sector. The economic damage from such data breaches can be catastrophic, with annual costs of cyber crime for the public sector averaging \$80 million.

Algorithms can be programmed to optimize multiple municipal services if given correct input from sensors. However, if sensors malfunction or aren't programmed correctly, sensitive data and civic reputations could be put at risk. Likewise, hackers and online criminals determined to steal sensitive data have an ever-increasing attack surface as more sensors are put into service.

It is critical for public entities to protect their digital assets by adopting effective IT security measures. Consider the following risk scenarios:

Sensitive data breach. To decrease hardware and administrative costs, a city stores sensitive data in a third-party cloud service. Some of the data stored are manual security override codes allowing city officials to enter buildings in the event of a power failure. A cyber thief breaks into the cloud, gaining access to the codes and uses them to enter the building where he steals city officials' credit card data. The city must pay engineers to fix the vulnerability, as well as a public relations firm to repair its damaged reputation for failure to secure sensitive data.

Programmer power error. At high-usage times throughout the summer, a city cannot generate enough of its own electric power due to high air-conditioner use. As a result, it has to buy power on the open energy market from other cities and transmit the electricity over third-party power cables. A computer algorithm is written to always buy power from the city with the least expensive bid. However, due to a programmer power error, the algorithm inadvertently chooses the most expensive bid, costing the city millions in overpayments of off-system electricity purchases.

Activist sympathizer. A radical activist group that disagrees with city policies stages a protest during the workweek. One of the city's IT workers sympathizes with the activists' aims and captures all web traffic to city internet sites and reroutes it to the activists' site in an attempt to gain publicity for the cause. Civic leaders must pay to add extra layers of security to city web servers and endure the embarrassment of having allowed their systems and proprietary information to be used in an unauthorized, and highly visible, way.



Property and collateral damage

Internet-connected sensors embedded into public infrastructure can help municipal operations run smoothly and effectively. However, if those sensors should fail, or if machine-to-machine communication operates incorrectly at the wrong time, it could result in damage to public or private property.

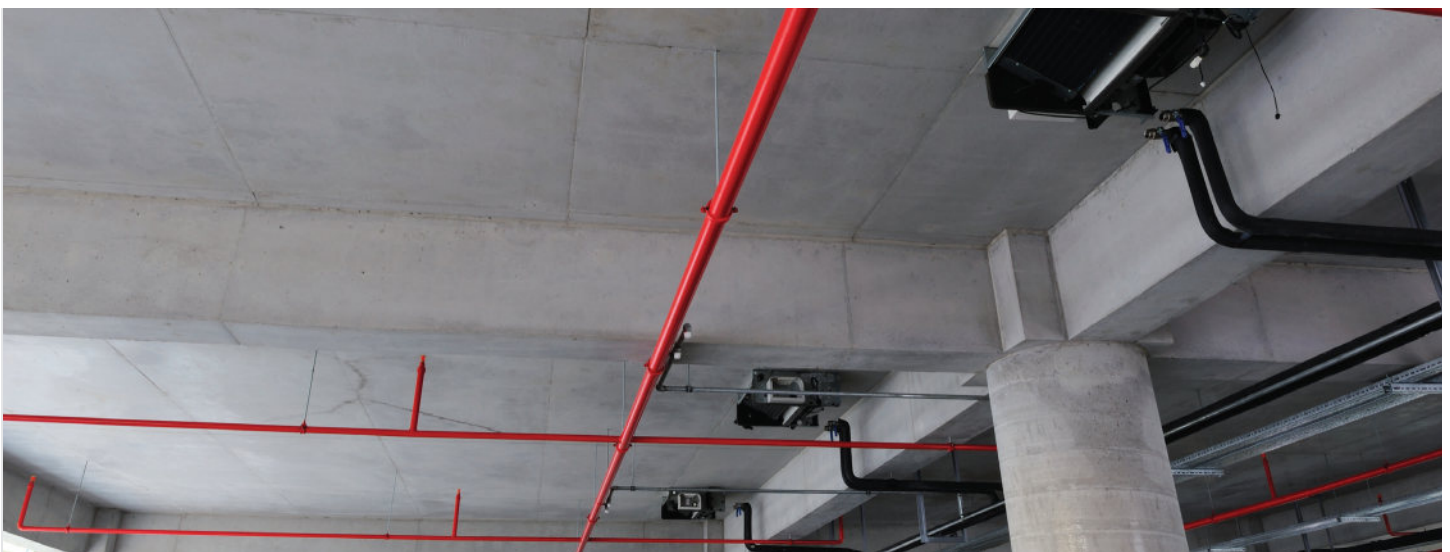
Property damage risk refers to the risk of the destruction of tangible property owned by the public entity. Collateral damage, on the other hand, refers to property owned by third parties that may have been damaged as the result of a city's action, such as an unexpected system outage or malfunction. In either case, such property can include real property, personal property and automobiles. If a public entity's newly installed "smart technology" causes property damage due to a defect or a failure to function as intended, a lawsuit could result and the public entity could be at risk.

ILLUSTRATIVE RISK SCENARIOS

Transformer fiasco. A cyber intruder gains entry into a city network through a vulnerability in a sensor not armed with anti-tampering features. The intruder releases a self-propagating worm that targets the city's electrical grid. The worm causes multiple transformers to blow, causing major fires in several areas of the city. Home and business owners affected by the fires sue the city for damage to their property as a result of failure to secure the vulnerable sensors.

Full-scale water tank failure. A city stores water tanks on top of municipal buildings that provide water to the building and, in some cases, adjacent buildings. But, when a defective sensor fails to do its job, mounting water pressure quickly causes a major water disaster. Had the sensors communicated properly with cloud-based warning systems, the costly leak and resulting property damage could have been avoided.

Theft of remarkable proportion. A midsized city has a building that houses valuable historical documents on loan from a private collector. To enhance security, city officials arm it with security sensors connected to the internet, along with cameras to monitor visitors and security personnel. One night, a thief gains entry into the building, but window sensors malfunction and fail to notify police. The thief steals historical documents and damages others while fleeing. The city is held responsible for the loss of the documents and damages.



Bodily injury

Even though a new smart technology may be thoroughly tested before it is sold to any public entity, defective sensors or software bugs still slip through to an end user. Other times, sensors may work properly, but human error in the analytic function can result in a malfunction leading to citizen injuries or worse.

When the physical well-being of citizens and visitors is at stake, civic leaders must take extra measures of care when planning and implementing smart technology. Failure to anticipate how things could go wrong may result in liability lawsuits, should an injury be traced back to a faulty sensor action or inaction.

ILLUSTRATIVE RISK SCENARIOS

Come drought or high water. A city relies on sensors and complex back-end systems to monitor flood and drought conditions. A sensor malfunctions and a road that frequently floods in the spring goes unreported to city officials. A vehicle hits the flood waters and veers into a guardrail. The citizen sues the city for bodily injury as a result of the road not being closed due to flooding.

Historic 5K fall. A city installs sensors to monitor the structural health of one of its landmarks – a historical, covered footbridge. The sensors fail to detect deterioration in the support beams in the months before the holiday 5K run. The bridge gives way as 20 athletes cross it simultaneously. The city and sensor manufacturer are sued for bodily injury to the runners.



Actions to consider for minimizing risk

Smart technology opens up a new world of possibilities for cities to perfect and streamline their services. The more we learn about the risks smart technology devices create, the more we should consider action to mitigate exposure to them. Consider the ways to protect citizens and visitors from the key risk scenarios on the previous pages.

NETWORK AND INFORMATION SECURITY

Maintain an asset inventory. Without full knowledge of the critical assets within an organization, protecting these assets with the appropriate controls to help mitigate losses will become a daunting task. Be sure to include people, processes and technologies when considering a full asset inventory.

Conduct a risk assessment. Conduct a risk assessment for each system under consideration that stores, processes or transmits confidential and/or sensitive information. Both deliberate and accidental cyber threats, and their potential impacts, must be examined, and all possible gaps in potential solutions should be documented.

Evaluate technology solution providers. Any contractor or solution provider under consideration should be properly evaluated for technical expertise. Make sure to verify all degrees, credentials and industry certifications of the providers who will actually be doing the work. Smart devices and systems often run 24/7 year-round, so outside consulting firms should provide an acceptable level of support around-the-clock. Verify that the hardware and equipment chosen adheres to sound industry design standards. All software should be written according to generally accepted security coding practices and patch protocols. Service-level agreements should be examined by qualified attorneys.

Implement vendor management. Industry best practices related to cybersecurity should be used when implementing policies and practices that support a sound vendor management program. Some examples include management of vendor remote access, identification and authorization of vendors to your systems. Ensure that vendors implement controls and safeguards if they store, process and/or transmit customer or third-party data on your behalf.

Balance contract language. Many public entities outsource their information systems management to outside IT firms. Quite often, the contracts that these firms offer will heavily favor the contracting firm as opposed to the public entity. Qualified legal counsel should review any potential contracts regarding service-level agreements and insist on language changes to protect the public entity's interests.

Evaluate cloud providers. External cloud service firms often employ highly trained certified administrators with high levels of experience in network and information security. But, these firms can still experience outages and security breaches. Public entities should specify security and encryption requirements and insist on understanding how cloud providers avoid co-mingling data with that of their other clients who share the same physical hardware. Be sure to understand the roles and responsibilities of the cloud service provider (CSP) in the event of a breach. Will they help with the investigation? How quickly will you be notified? How would you retrieve your information if the CSP went out of business or was breached? Do you have another means by which to conduct your business or do you rely solely on the CSP for business-critical functions?

Automate security monitoring. 24/7 security monitoring is crucial to safeguarding complex connected systems. Any system installed should include a section where city IT leaders can configure custom alerts to respond to any unusual network activity in real time; those alerts should be evaluated and updated regularly. Threats to network, power, storage, servers or mission-critical applications must be dealt with immediately by qualified administrators and programmers to prevent unexpected downtime.

Identify technology interdependencies. Because technology initiatives are project based, many leaders feel that the technological components of one project are separate and distinct from others. However, many of these projects share code modules and executable applications for mission-critical operation, so changes in one project may have negative consequences for another. Trained systems analysts should identify the cyclical dependencies between hardware and software systems to make sure which applications can be changed without adversely affecting others.

Enforce smart IT department policies. Ensure that users adhere to strong password policies and rotate employee-assigned security keys to ensure that terminated employees' IT privileges can be decommissioned at appropriate times. You should also modify the privacy and security settings of devices to comply with security policies. And, remember to establish appropriate bring your own device (BYOD) policies and put measures in place to verify employee compliance.

Maintain computer equipment. Because computers have few visible moving parts, supervisors and their staff tend to overlook the fact that they require maintenance like other publicly owned and operated equipment. Every day, public entities are coming to rely more heavily on computers to deliver mission-critical municipal services. Extended downtime will prevent a public entity from keeping its citizens and visitors secure from the spectrum of threats it faces every day. On-premises servers should be kept in modern data centers that are temperature-controlled and secured from unauthorized entry. Implement a patch management program that, at minimum, meets industry best practices.

Promote security awareness. Sometimes the biggest threat to your environment can come from within, most times with no ill intentions. If employees are not trained periodically on how to safeguard confidential/sensitive data, are not cognizant of phishing attempts and hacking techniques or not generally aware of other forms of data protection, the entity increases its risk exposure.

Continuously recruit IT talent. Civic hiring authorities must understand that experienced technicians are in high demand and short supply. As a result, experienced workers may not be available at the time they're needed. Also, IT employees change jobs more often than other non-technical workers, so public entities should plan for adequate funding to recruit and train personnel to repair smart systems from various vendors. Recruiting efforts should not stop simply because there are no open job orders. Consider planning for more frequent employee turnover among valuable knowledge workers.



ORGANIZATIONAL AND COMMUNITY READINESS

Develop a continuity-of-operations plan. In a disaster recovery or emergency response situation, operational continuity of government functions is vital. Have a plan in place and accessible even if smart technology is largely unavailable or offline, and consider the following: How are employees paid? Do fire trucks and ambulances have enough gasoline? Do rescue teams have the tools they need to function effectively?

Establish low-tech contingency plans. Many smart technology communications can come to a halt in the event of a citywide outage or a large-scale cyber attack. This could force computer-regulated municipal systems offline, resulting in entire departments becoming inoperable. Leaders should develop contingency plans to operate mission-critical services in a low-tech mode for as long as necessary until automated systems can be restored. For example, officers accustomed to having tablet computers in their police cruisers should be required to undergo instruction on how to do their jobs effectively without them in the event of a prolonged system outage.

Invest in backup power systems. An uninterruptible power supply (UPS) has become the industry standard in the technology sector to maintain power flow if the region's main generators go down. Have IT leaders establish contingency plans and train their personnel with scheduled drills so that everyone knows what to do in the case of a widespread outage and understands how long backup power supplies can operate.

Invest in employee decision-making training. Smart technology relies on computer algorithms to make pre-programmed decisions based on sensory input. However, it is ultimately the human operators who make the final decisions on how the technology-enabled equipment should react. Civic risk management often focuses too much on the equipment being controlled and the processes in place rather than the government employees who operate the equipment. Consider investing in situational, case-oriented training for human operators and encourage them to speak up if they notice a potentially dangerous situation that could cause bodily injury or property damage.

Proactively earn public trust. In this age of growing cyber threats, state and local governments must publicly demonstrate that they understand the sensitive nature of personal data and that they're taking the precautions necessary to ensure security. With now-ubiquitous technology, government leaders should carefully consider the data under their management and provide the public with a plan to safeguard the systems that serve the community.



Insurance considerations

Cities are boldly taking the initiative to operate their civic services with computer automation, machine-to-machine communication and the Internet of Things (IoT). Never before have cities had so much innovation to keep life within their boundaries safe and secure. As we've seen, the benefits of this technology can greatly increase a city's appeal.

However, these new types of automation also bring risks that many public entities have never encountered before. As a result, it's impossible to predict all the ways in which cities could be liable should systems fail to operate as expected. While this risk cannot be eliminated, it can – and must – be managed.

To help decrease exposure, public entities should investigate their insurance options for the categories of risk described in this issue of the Public Sector Risk Advisor. The following table recounts the illustrative risk categories and the relevant insurance coverage to protect against liability.

Risk category	Illustrative risk scenarios	Relevant insurance coverage to evaluate with an agent or broker
Cyber	<ul style="list-style-type: none"> • Sensitive data breach • Programmer power error • Activist sympathizer 	<p>Information security insurance provides coverage for critical cyber risks. Coverage options vary, but most include network and information security liability. Companies can also opt for many first-party expense reimbursement coverages, including data restoration, extortion, social engineering, business interruption, computer and funds transfer fraud, crisis management, and security-breach notification expenses.</p>
Property and collateral damage	<ul style="list-style-type: none"> • Transformer fiasco • Full-scale water tank failure • Theft of remarkable proportion 	<p>Property insurance provides coverage for buildings, business personal property, loss of business income and extra expense.</p> <p>Auto liability insurance provides coverage for bodily injury and property damage caused by a covered auto.</p> <p>Auto physical damage insurance provides coverage for physical damage to owned autos, including coverage for audio and radar detection equipment (if part of normal inventory of the vehicle), air bags and customized equipment attached to an emergency vehicle or public transportation auto.</p>
Bodily injury	<ul style="list-style-type: none"> • Come drought or high water • Historic 5K fall 	<p>General liability insurance provides coverage for damages for bodily injury to third parties for which the insured is legally liable.</p>



Each city's security requirements are unique, so few insurance policies come standard and not all risks may be insurable. It's important to contact your independent insurance broker to discuss your city's specific insurance needs.

How Travelers can help

Travelers understands the unique challenges municipalities and counties face every day. Our Public Sector Services group has focused on public entities since 1991. They stay ahead of the risks these entities face – from cyber risk to law enforcement liability – and provide them with the coverage and service they need.

So, whether you're evaluating municipal surveillance technology, smart street lighting or even crime simulation modeling, you can trust Travelers to provide insights and effective insurance solutions to manage the risks tomorrow's emerging technology will bring.

For more information, contact your independent insurance agent or visit us on the web at travelers.com/publicsector.



SOURCES

¹ Meyers, M., Niche, C., Eggers, W., “Anticipate, Sense, and Respond: Connected Government and the Internet of Things,” Deloitte University Press, 2015, accessed Jul 2016, <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology/iot-public-sector.pdf>

² McGraw, Mike, “A City Haunted by Ghost Water: Leaking Water Adds Millions to Ratepayers’ Bills,” Flatland, 2017, accessed Jun 2016, <https://www.flatlandkc.org/public-works/overviews-introductions-public-works/digging-in/city-haunted-ghost-water/>

³ “What is the Smart Grid?” U.S. Department of Energy, 2016, accessed Jun 2016, https://www.smartgrid.gov/the_smart_grid/smart_grid.html

⁴ “Modernizing Hawai’i’s Grid For Our Customers,” Hawaiian Electric, Maui Electric, Hawaii Electric Light, 2017, accessed Jun 2018, <http://www.mauismartgrid.com/how-will-smart-grid-technologies-improve-mauis-energy-system/>

⁵ “Idaho Falls Power Smart Grid,” Idaho Falls Power, 2016, accessed Jun 2018, <https://www.smartgrid.gov/files/TPR11IdahoFallsPowerSiteTests.pdf>

⁶ Davis, Kathleen Wolf, “A Con Edison Viewpoint: Phoning In Stray Voltage Detection,” Energy Central, Apr 2013, accessed Jul 2018, <https://www.energycentral.com/c/iiu/con-edison-viewpoint-phoning-stray-voltage-detection>

⁷ “IDC MarketScape: Worldwide Smart Building Energy Analytics 2011 Vendor Assessment,” IDC Energy Insights, 2011, accessed Apr 2019, <ftp://public.dhe.ibm.com/software/emea/de/tivoli/IDC-Smart-Buildings-Energy-Analytics-study.pdf>



Travelers Public Sector Services



[travelers.com](https://www.travelers.com)

The Travelers Indemnity Company and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material is for informational purposes only. All statements herein are subject to the provisions, exclusions and conditions of the applicable policy. For an actual description of all coverages, terms and conditions, refer to the insurance policy. Coverages are subject to individual insureds meeting our underwriting qualifications and to state availability.

© 2019 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. BPSWH.0007 New 4-19