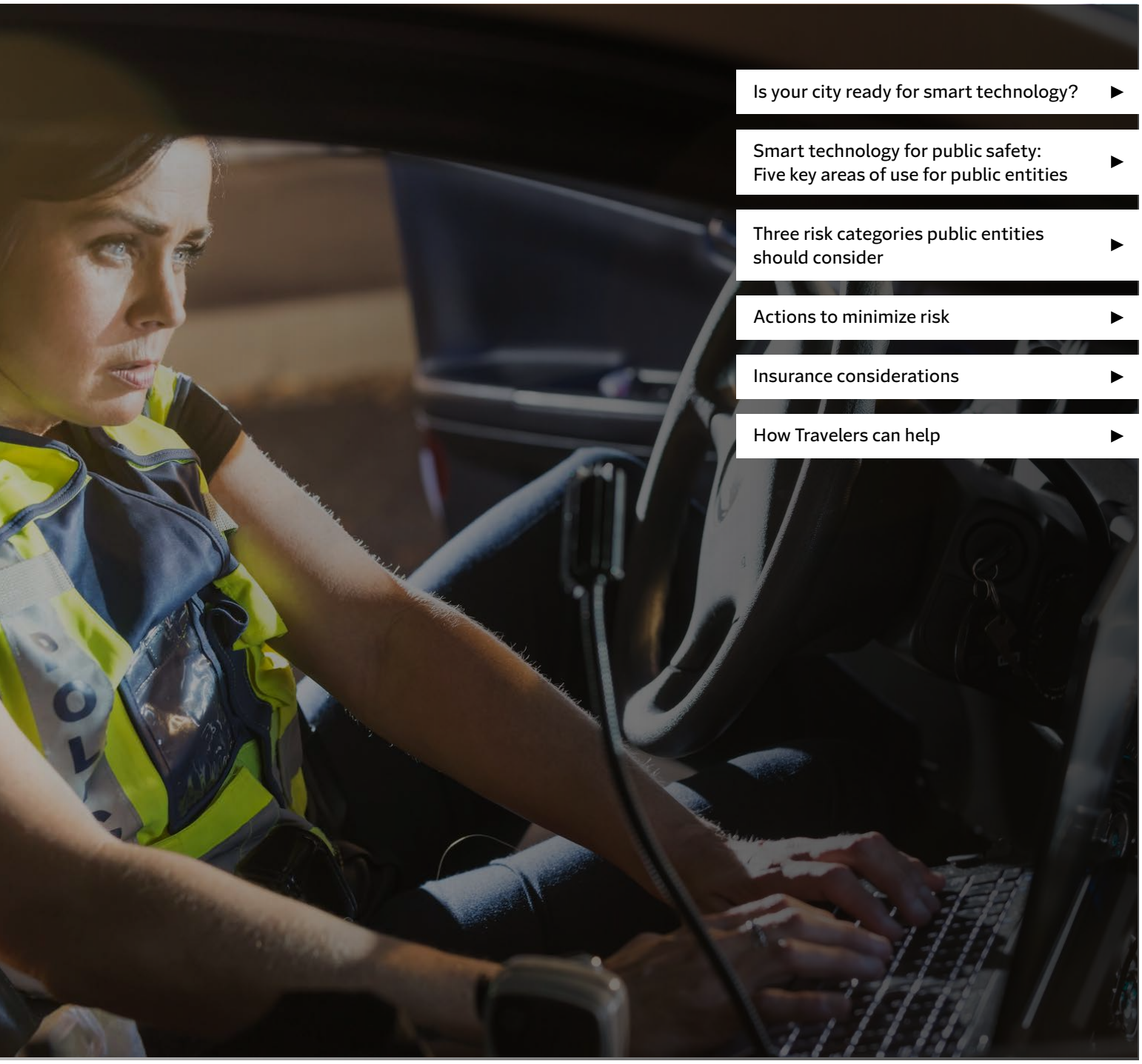
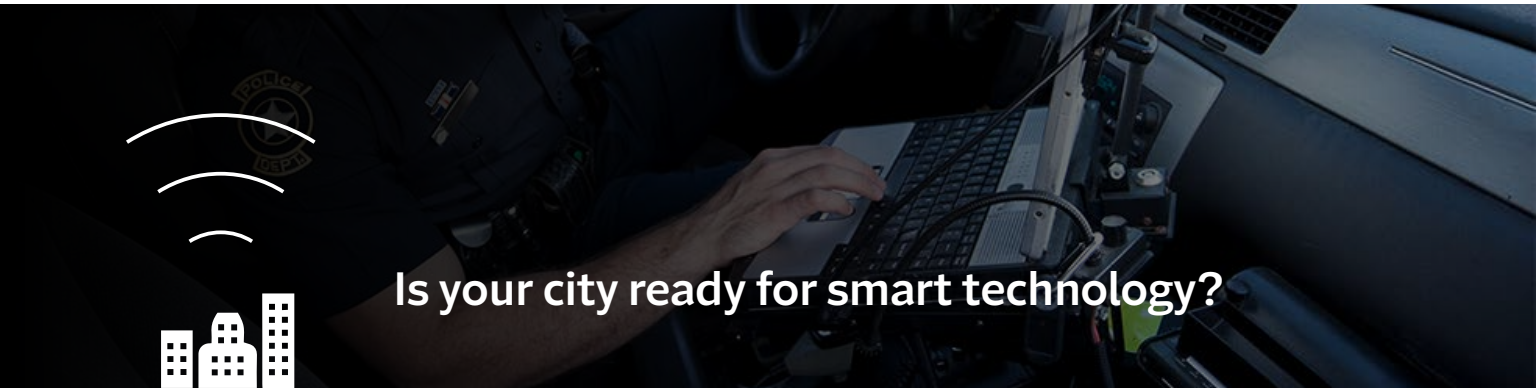
TRAVELERS

TRAVELERS PUBLIC SECTOR SERVICES
RISK ADVISOR SERIES



Public safety for the smart city

INSIGHTS FOR PUBLIC ENTITIES ON MANAGING THE RISKS OF SMART TECHNOLOGY FOR PUBLIC SAFETY



Is your city ready for smart technology?

Civic leaders face a multitude of challenges, including planning for public safety within the communities they serve. Mayors, public risk managers and city council members need to take steps to keep citizens safe on the streets and children safe in public schools. These are two foundational concerns for cities, often accounting for a significant portion of budgets and attention.

New smart-city technology is emerging to help cities fulfill their public safety obligations, and many municipalities are increasingly leveraging its power. Tech-savvy civic leaders routinely use automated decision support systems to serve their constituents more effectively. New Internet of Things (IoT) devices are playing an important role in public safety initiatives. Machine-to-machine communication streams data to and from control centers with little or no human interaction. Big data allows city managers to make better safety decisions faster.

These technological breakthroughs are transforming urban landscapes and helping to improve the quality of life of residents, business owners and visitors – and they're delivering efficiency gains that help municipalities cut costs over time. But with increased technology comes increased risk. Public entities should understand these risks and take steps to prepare.

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.

"The purpose of government is to enable the people of a nation to live in safety and happiness." Thomas Jefferson

Smart technology for public safety:

FIVE KEY AREAS OF USE FOR PUBLIC ENTITIES

Protecting the safety of residents, visitors and the public at large has long been a core responsibility of local, state and national governments. As technology evolves and becomes more affordable, new and innovative ways emerge for governments at the city and county levels to monitor and protect the safety of those communities.

These "smart technology" solutions for public safety are varied, ranging from body-worn cameras for law enforcement officers to record video and audio surveillance, to smart streetlight systems in parks and neighborhoods. Ultimately, these technologies can be interconnected to form a framework of devices and software, including sensors and IoT devices, that offer new and innovative ways for local governments to protect public safety and maintain or improve the quality of life within their jurisdictions.

In the pages that follow, we explore several ways in which cities and other public entities are using smart technology to enhance public safety. Then, we explore key risk categories impacting the cities that deploy this technology and highlight specific actions to minimize risk. Finally, we share insurance considerations that public entities should discuss with their independent agent or broker.

1.
BODY-WORN CAMERA SYSTEMS

Body-worn cameras are at the center of a debate that isn't likely to subside in the near future. Recent high-profile cases have included both video evidence from officer-worn body cameras and cellphone video from citizens observing the incident. This trend has shone a spotlight on body-worn camera technology and its use.

Many law enforcement agencies and local governments now require wearable video recording devices. This widespread push has prompted the development of new, enhanced capabilities for body-worn cameras that do more than capture video footage, such as:

- Streaming video and transferring video data to a police, command or dispatch center.
- Voice-to-text software that automatically transcribes audio captured by the camera.
- Automatic video activation when an officer opens a vehicle door, is running or goes down in the call of duty, or enters a predefined geographical area.
- Smart sensors that detect when a firearm is removed from its holster activate the camera and send real-time alerts to dispatch nearby officers. The emergence of body-worn cameras has led local governments to adopt policies that govern their use and specify how and when device recordings can be released publicly following an incident. It is critical for law enforcement professionals to find ways to educate officers and their communities about these department policies. It's also important for officers to understand that many of their public interactions will now be recorded – not only by the devices they are wearing, but also by the citizens they encounter during their shifts.

As body cameras become more widely used across the country, there is the potential opportunity to use footage from cameras as a training tool to help officers better understand interactions with citizens, the techniques utilized and their real-world outcomes. This capability is significantly altering officer training.

2.
SMART VIDEO AND AUDIO SURVEILLANCE

Since the late 1960s, law enforcement agencies in the United States have been using video surveillance to deter crime and assist in prosecutions. Video technology has evolved over the years, but most surveillance systems remain inefficient. Blind spots in video networks, low-quality imagery and slow data retrieval can hamper authorities' efforts to protect their citizens. Recently, however, surveillance has taken a giant leap forward with both video and audio capabilities.

Smart cameras combine video with analytics software, equipping cities with the ability to respond to evolving situations, research public safety trends and review footage stored in the cloud. When deployed at strategic locations throughout a city, smart cameras can serve many valuable functions.

For example, they can:

- Identify accidents as they unfold and call for emergency services.
- Provide data to help manage traffic flow, making streets safer for drivers, residents and businesses.
- Read license plates.
- Help solve crime. Law enforcement can review video footage to find suspects or identify higher pedestrian traffic to help pinpoint which neighborhood property may be a potential drug den.

Surveillance isn't limited to just video. Gunshot detection systems use acoustic sensing technology to help identify and report gunshots to the police within seconds of a shot being fired. More than 100 U.S. cities employ this technology to help monitor high-crime neighborhoods and respond quickly when gunfire is detected.[1]

Acoustic sensors can also recognize sounds that are often connected with a threat, such as breaking glass or shouting. Municipalities can respond proactively, before dangerous situations get worse.

[1] http://www.icjia.state.il.us/assets/articles/Shotspotter-Final-191213T18420528.pdf

3.
SMART STREET LIGHTING SYSTEMS

Nothing deters crime like visibility. Street lighting is often the first smart technology that cities address because of its potential to reduce energy consumption. Super-efficient light-emitting diode (LED) bulbs last longer and produce two to three times more light per wattage than legacy bulbs. Falling prices for LED lights have led many cities to transition to this more controllable lamp technology.

LED-based smart street lighting incorporates various technologies, such as cameras, light-sensing photocells and other sensors that enable adaptive lighting and real-time monitoring. As a result, streetlights can:

- Brighten or dim automatically based on lighting conditions or through remote control.
- Respond dynamically to movement, providing as-needed illumination that discourages crime and improves visibility, safety and comfort for pedestrians, drivers and businesses.
- Flash warning signals that adjust to daylight levels in the event of an emergency. Additional sensors and software applications can provide even more smart streetlight functionality, including the ability to:
  - Monitor traffic, pedestrians and parking. Public entities can use this critical data to make decisions about public safety personnel and plan for future infrastructure, traffic control and more.
  - Proactively alert city operations of lamp outages and failures, allowing public safety employees and utilities to address problems faster and reduce maintenance costs.

Smart streetlights really aren't just lighting anymore – they are data collection hubs that can be placed throughout a city or town. They can also serve as the entry point for an entire smart-city network.

4.
BIOMETRIC MONITORING SYSTEMS

Biometric technology can identify people based on their unique biological characteristics. Some biometric instruments identify fingerprints and facial features. More advanced devices can detect iris patterns, gaits, voice prints, DNA and even human thermal signatures.

Most biometric systems work in a similar way. Sensors collect the person's biometric information and back-end systems then compare that data to a centralized database of known individuals for positive identification. A match can help to verify a person's identity, reveal the identity of an unknown person, or pinpoint someone on a watch list of known or suspected terrorists.

Law enforcement has long taken advantage of biometrics – and they're benefiting from recent advances as well:

- Police routinely collect DNA and fingerprints at a crime scene.
- Prisons can use high-resolution iris images to identify new prison inmates with greater accuracy than the traditional fingerprint.
- Live face recognition has gained interest for public security purposes. Federal law enforcement and state and local police use facial recognition technology to assist in thwarting criminal activities. Security personnel can use this technology to scan a crowd and identify someone who may be a threat.

Biometric identification techniques have the potential to dramatically improve security and help identify criminals, but privacy is a significant concern. Biometrics can be stolen, shared or sold, creating the risk of identity-based attacks over which people have no control. Unlike a password or credit card, biometrics can't be changed. Facial recognition systems pose a particular risk because they can be used for general surveillance without a person's knowledge or consent.

Many state and local governments regulate the collection, use and retention of biometric data, and this trend is growing across the country. The most notable is the Illinois Biometric Information Privacy Act (BIPA), which requires organizations doing business in Illinois to implement policies regarding retention of biometric data.

5.
EMERGENCY AND EXTREME WEATHER RESPONSE

High-profile emergencies and weather catastrophes have given Americans a new appreciation for emergency response capabilities. Police, fire, medical and other first responders have shown bravery beyond measure as they risk their own lives to save others. Smart cities are augmenting these vital human services with technology that takes emergency response to the next level, helping to better predict, prepare and respond to disasters in real time.

Using connected sensors, smart cities can record even minor changes to normal conditions, such as air quality and water levels, and highlight potential trouble areas on a centralized dashboard. Machine-learning technology can then evaluate the risk of damage and alert the authorities who are in a position to respond.

Here are some of the ways smart-city technology supports emergency preparedness and response:

- **Electrical grid.** Smart grids monitor, measure and manage the transport of electricity using advanced computer systems, wireless networks and sensors along transmission lines. In the event of an emergency or disaster, the grid automatically notifies city leaders and utilities of power outages in real time, allowing them to more quickly isolate problems and restore service to customers.
- **Transportation.** Smart traffic lights give priority to authorized emergency services like the police, fire department and ambulance services, saving precious time when life and property are at stake. Other smart transportation systems make it possible to alert drivers of potentially hazardous situations ahead. They can evaluate road and weather conditions and redirect traffic to the safest and most expedient route, as well as monitor the structural health of bridges and other structures.
- **Environmental management.** Sensors perform a number of functions to ensure a safe physical environment:
  - Monitor water levels for drought and flood, identify pipeline leaks and predict equipment failure.
  - Detect water and air pollution that could endanger residents and emergency responders.
  - Measure sewage system overflows.

  Normalizing these essential functions after a natural disaster is vital to keeping a city habitable.
- **City services.** Smart snowplows and salt trucks can track when streets have been cleared and notify residents and city employees electronically.

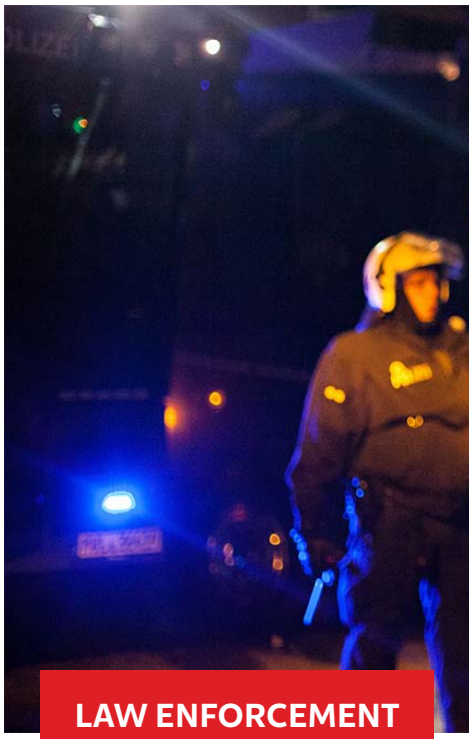
Communication is vital in warning communities of emergencies and severe weather events and facilitating an effective response. IPAWS, or Integrated Public Alert and Warning System, is a FEMA-driven initiative that provides alerts to the mobile devices of citizens so they know when severe weather, or other hazards, are in the area. Use of such technology can not only keep the public safe, but could also reduce the number and severity of emergency calls to first responders, helping to keep them less exposed when extreme weather is a threat.

A Team Awareness Kit (TAK) is another digital tool that can significantly improve safety for first responders. It enables easier communication across jurisdictions by providing a common platform where responders from multiple agencies can all communicate and have their locations tracked in a single system. This greatly reduces on-scene communication difficulties and helps allocate resources quickly and efficiently where they are most needed.

Three risk categories public entities should consider

Smart technology offers cities new ways to enhance public safety and law enforcement capabilities, as well as enhance convenience and productivity. They also may pose unintended risks, especially if policies, procedures and training practices do not adequately address new capabilities. Any public entity contemplating the adoption of smart devices and technology should consider the following three related categories of risk:

CYBER



LAW ENFORCEMENT LIABILITY

BODILY INJURY

Cyber

Cyber is a major concern for public entities, and the risk grows as cities expand their use of smart technology. State and local governments are top targets for cyberattacks, which can cause significant damage. Vital services such as electricity and water may be compromised. Citizens' sensitive personal information may be captured and misused. Ransomware is an ever-increasing threat, with nearly half of all ransomware attacks targeting municipalities. Successful attacks can bring municipal operations to a halt until payment is made and have a direct financial impact on the municipality's ability to function.

As of 2021, global data breaches cost $4.24 million, on average.[2] Ransomware costs averaged $4.62 million[3], and there's no end in sight. Every year cyber threats are growing in number and costs as cybercriminals and phishing schemes become increasingly sophisticated.

That's why it is so important for public entities to protect their digital assets with effective cybersecurity measures. Consider the following risk scenarios.

[2,3] Cost of Data a Breach Report 2021

ILLUSTRATIVE RISK SCENARIOS

- **International stolen ID.** A law enforcement agency's computer network is compromised by a virus, which allows foreign hackers to steal personally identifiable information (driver names, addresses, dates of birth and Social Security numbers), as well as videos obtained from traffic incidents captured on body-worn camera video. The law enforcement agency pays more than $125,000 to recover from the breach, which includes investigating and eradicating the virus, and sending breach notifications to those affected with an offer of free credit monitoring and call center support.
- **Child safety database.** As part of a new child safety program, city officials install a biometric system that allows parents to voluntarily store their children's fingerprints and photos in a database for future reference. A hacker gains entry to the system through a loophole in the system's software and distributes the data on the internet. The city is sued by the parents for lack of adequate protocols to protect children's personal biometric data.
- **Ransomware storm cloud.** Just prior to hurricane season, a city in the southeastern United States installs a smart emergency response system for coordinating local and state resources in the event of extreme weather. Six weeks later, as a massive tropical storm develops in the Gulf of Mexico, a municipal employee opens an email that installs a ransomware virus onto the city's new emergency response system. The ransomware allows a criminal group identifying itself as "StormCloud" to encrypt and hold hostage files and system elements critical to the proper functioning of the emergency response system. StormCloud demands a six-figure ransom, payable in bitcoin, in return for a decryption key to reverse the problem. As the tropical storm picks up speed and gets closer to landfall, the city council votes to pay the ransom. Later, the city incurs additional expenses to investigate whether the ransomware has impacted other municipal systems.

What is ransomware and how can multifactor authentication (MFA) help reduce the likelihood of a successful ransomware event?

Ransomware is malicious software that either locks up a computer or its data until a ransom is paid. The data held hostage is encrypted, preventing users from accessing files, databases or applications. Once the virus is activated, the victim typically receives a message from the hacker, who demands a payment in exchange for a decryption key that releases the locked data.

Cybercriminals often launch a ransomware attack and gain access to a network with phishing attempts that implant password-stealing malware or trick users into exposing login credentials. MFA can minimize the success of these tactics. With MFA, users must supply two or more pieces of information when logging in to a network, such as a password plus the correct answer to a security question or a code sent to their mobile phone. Hackers may gain possession of employee passwords, but they're unlikely to have access to the additional factors required to log in. This can greatly reduce the risk of a successful ransomware event.

Law enforcement liability

In the course of doing their jobs, law enforcement personnel could be accused of wrongful acts resulting in lawsuits for bodily injury, false imprisonment or excessive use of force. Because many officers now utilize body-worn cameras, there may also be invasion of privacy claims, depending on the circumstances of the case. Likewise, cities may find themselves facing more lawsuits alleging liability for damages if biometric systems or similar technologies fail to perform as intended.

ILLUSTRATIVE RISK SCENARIOS

- **Firecracker versus gunshot?** As a result of increased criminal activity, law enforcement has installed gunshot surveillance systems throughout the city. Late one summer night, a few teens decided to light firecrackers in one of the abandoned alleyways, setting off the gunshot surveillance sensors. When the police arrived on the scene, they arrested the teens for reckless endangerment, believing that the teens had fired weapons.
- **Doppelgänger dilemma.** A city deploys special facial recognition at a local stadium just prior to a high-profile professional sports event. The system compares attendees' faces with those of wanted criminal suspects. The system incorrectly identifies one attendee as a dangerous criminal suspect, based on the system's matching algorithm. Law enforcement personnel immediately apprehend the suspect, using pepper spray when the person responds combatively. Local law enforcement later discovers the identification error. The fan sues for false arrest and bodily injury.
- **Body-worn camera redaction error.** Several police officers equipped with body-worn cameras respond to the scene of an alleged assault involving a group of young males. The city's police department receives Freedom of Information Act (FOIA) requests from media outlets seeking footage of the police response to the event. The city's police department uses new video redaction software to redact the faces of innocent bystanders. They erroneously fail to redact one innocent bystander's face. Media outlets widely distribute the footage indicating it shows those involved in the assault. The unredacted innocent bystander is publicly identified as a potential criminal, resulting in emotional distress, harassment on social media and in public, as well as the loss of his employment. He files suit against the department and multiple media entities seeking monetary damages.

Bodily Injury

Smart technologies rely on electricity and wireless communication to exchange digital signals in the field. They may be thoroughly tested, but defective sensors and software may slip through or properly functioning sensors may malfunction over time. Civic leaders should be aware of how a faulty connection or damaged smart technology may lead to liabilities.

ILLUSTRATIVE RISK SCENARIOS

- **Flood sensor failure.** A coastal city relies on sensors strategically placed within the city sewer system to detect flood conditions and notify service crews. The city failed to properly maintain the sensors, and some sensors are no longer properly secured to their moorings. During a tropical storm, fast-moving water physically dislodges the sensors from their moorings, so service crews are never notified. Debris collects in the storm drains, causing a flash flood that catches citizens off guard. People are swept away in the torrential rains, and the city is sued for bodily injury caused by its failure to detect rushing water.
- **Icy conditions misreported.** A midsized northern city enhances its winter weather response capabilities by integrating sensors into trucks and plows used for snow removal. The sensors connect to a new public website that reports on snow removal and road conditions. During a mid-January blizzard, the sensors fail to work as intended, and the city's website inaccurately reports that a town property has been cleared. After checking conditions online, a third party arrives on the scene, slips on a patch of ice and suffers a ruptured disk in his spine. He files a slip-and-fall lawsuit against the city for negligence and premises liability.

Actions to minimize risk

For cities and other public entities looking to upgrade their public safety capabilities, smart technology can pose unintended risks. Fortunately, there are ways to mitigate these risks.

Any public entity considering using smart technologies should consider the following actions related to network and information security, law enforcement policies and procedures, and organizational and community readiness.

Network and Information Security

- **Maintain an asset inventory.** Full knowledge of the critical assets within an organization is a vital first step to protecting them with the appropriate controls. Be sure to include people, processes and technologies when building a complete 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. Consider both deliberate and accidental cyber threats and their potential impacts, documenting all possible gaps in potential solutions.
- **Implement vendor management.** Work with all suppliers, vendors and cloud providers to create a security-first culture. Require them to maintain, at a minimum, the same security standards that your organization maintains. When contracting cloud providers, be sure you understand their security requirements and how they will avoid commingling data with that of other clients who share the same physical hardware.
- **Balance contract language.** When entering into an agreement with vendors or outside IT firms, always require qualified legal counsel to review any potential contracts or service-level agreements the firm offers. Insist on balanced language that protects the interests of the public entity as well as the outside firm.
- **Automate security monitoring.** 24/7 security monitoring is crucial to safeguarding complex connected systems. Any smart system should allow city IT leaders to configure custom alerts to respond to any unusual network activity in real time. Qualified administrators and programmers should respond immediately to threats to network, power, storage, servers or crucial applications.
- **Identify technology interdependencies.** Because technology initiatives are project-based, leaders often feel that the technological components of one project are separate and distinct from others. However, many projects share code modules and executable applications that are vital for 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 ensure applications can be changed without adversely affecting others.
- **Have good defenses against cybercriminals.** MFA is recommended as a way to prohibit unauthorized users from accessing a network. MFA requires users to supply two or more pieces of evidence when logging in, which makes identity theft more difficult and can render stolen credentials less fruitful. Municipalities can also benefit from upgrading to endpoint detection and response (EDR), a security solution that continuously monitors all endpoints on a network, from computers and phones to servers and printers. If suspicious activity is detected, the EDR solution will take remedial action before the rest of the network is exposed.

- **Back up files daily.** Backups are essential to protecting cities from the effects of ransomware. Make frequent, comprehensive backups of all important files. Store backups offline, separately from the working network.
- **Maintain computer equipment.** Every day public entities are coming to rely more heavily on technology to deliver essential municipal services. Extended downtime will render a public entity unable to perform its mission of keeping its citizens and visitors safe. Always keep on-premises servers in a temperature-controlled environment that is secured from unauthorized entry. Implement a patch management program that, at a minimum, meets industry best practices. Monitor for security vulnerabilities in every platform being used, and make sure that the most current updates are installed. Have effective strategies for securing older versions of software that are no longer supported with patches.
- **Promote security awareness.** Sometimes the biggest threat to your environment can come from within, often with no ill intentions. To minimize the risk of exposure, train new employees and periodically refresh existing employees' knowledge on how to safeguard confidential/sensitive data, avoid phishing attempts, and be generally cognizant of all facets of data protection.
- **Continuously recruit IT talent.** Experienced technicians are in high demand and short supply. As a result, municipalities may find that experienced workers are not available when they are needed. Plan for adequate time and funding to recruit and train personnel to maintain all smart systems, even when there are no open positions.

Law Enforcement Policies and Procedures

- **Prepare for new law enforcement policies and procedures through training and modernization.** Public entities should update policies and procedures to reflect new technology implementations or service-level changes, and also provide the necessary training to promote their effective implementation. In addition, any updated policies and procedures should be reviewed by an attorney knowledgeable in law enforcement.
- **Preserve evidence for the chain of custody.** After implementing smart technology that records evidence digitally, make sure to archive data, including with a separated backup, and document evidence in a manner that is acceptable in court. Preserving digital evidence may involve methods that are completely different from traditional methods.
- **Address body-worn camera privacy concerns.** Protect the privacy of recorded data with strategies that preserve the evidence and prevent tampering. Specify when videos will be downloaded from the camera to storage and by whom. Identify who will have access to stored data, and maintain an audit trail of who accesses it, when and for what purpose. Establish appropriate retention policies for both evidentiary and non-evidentiary footage. The longer that recorded videos are retained, the longer they are subject to the risk of inadvertent public disclosure.

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. Just like making sure employees are paid, fire trucks and ambulances have enough gasoline, and rescue teams have the tools they need to function effectively, a continuity plan needs to be in place and accessible should the smart technology be largely unavailable or offline.
- **Establish low-tech contingency plans.** Smart technology communications can come to a halt in the event of a citywide outage or a large-scale cyberattack, which could take entire departments and computer-regulated municipal systems offline. 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 using software for fingerprinting or facial recognition, or having tablet computers in their police cruisers should be instructed on how to do their jobs effectively without them in the event of a prolonged system outage.
- **Invest in backup power systems**. 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 event of a widespread outage.
- **Invest in employee decision-making training.** Smart technology can rely on computer algorithms to make preprogrammed decisions based on sensory input. However, in many cases, the human operators make the final decisions on how to react to information from the technology-enabled equipment. Civic risk management may focus too much on installing or implementing smart technology, rather than the processes in place for the government employees interacting with it. Consider investing in situational case-oriented training for human operators and encourage them to speak up when they notice a potentially dangerous situation that could cause bodily injury or property damage.
- **Proactively earn public trust.** In our age of growing cyber threats, state and local governments must publicly demonstrate that they understand the potential sensitive nature of smart technology and that they are taking the precautions necessary to address these concerns. With now-ubiquitous technology, government leaders should provide public transparency for how they plan to use smart technology and address related concerns.

Insurance considerations

While public entities can take action to minimize their exposure to risk from new smart technologies, not even the most conscientious or well prepared can completely eliminate the significant risks. Each new public safety software system or connected IoT device introduces new uncertainties.

To help manage these risks, public entities should investigate the insurance options for the categories of risk. The following table recounts the risk categories noted in the previous section, the corresponding illustrative risk scenarios and the relevant insurance coverages that may assist public entities in protecting against potential loss.

RISK CATEGORY	ILLUSTRATIVE RISK SCENARIOS	RELEVANT INSURANCE COVERAGE TO EVALUATE WITH AN AGENT OR BROKER
Cyber	• International stolen ID • Child safety database • Ransomware storm cloud	Cyber insurance provides coverage for critical cyber risks. Coverage options vary, but most include network and information security liability. Entities can also opt for many first-party expense reimbursement coverages, including data restoration, business interruption loss, computer fraud, funds transfer fraud, e-commerce (cyber) extortion, crisis management and security breach notification expenses.
Law enforcement liability	• Firecracker versus gunshot? • Doppelgänger dilemma • Body-worn camera redaction error	Law enforcement liability insurance provides coverage for bodily injury, personal injury or property damage caused by a wrongful act committed while conducting law enforcement activities or operations.
Bodily injury	• Flood sensor failure • Icy conditions misreported	General liability and workers compensation insurance provide coverage for bodily injuries for which the insured is legally liable.

Each public entity's insurance requirements are unique. Insurance policies vary across carriers, and not all risks may be insurable. It is important to contact your independent insurance agent to discuss your unique insurance needs.

How Travelers can help

Since 1991, Travelers Public Sector Services has focused exclusively on public entities. We understand the unique challenges municipalities and counties face every day. Whether you are evaluating smart streetlighting systems or connected body-worn cameras, you can trust Travelers to provide insights and effective insurance solutions to manage the risks behind tomorrow's emerging technology.

Travelers stays ahead of public entity risk. For more information, contact your independent insurance agent or visit us at travelers.com/publicsector.

TRAVELERS PUBLIC SECTOR SERVICES

TRAVELERS

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.

© 2022 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.0004 Rev. 5-22