

# Becoming a smarter city: Six public safety projects that deliver quick results



## Contents

- 2 Executive summary
- 3 Introduction
- 4 Protecting public rail and other transportation systems
- 6 Defending city streets against criminal and terrorist acts
- 8 Lowering security costs while strengthening protection
- 9 Securing confidential systems and information from unauthorized access
- 10 Maintaining access to critical information and services when disaster strikes
- 12 Protecting citizens with faster and more coordinated crisis response
- 14 Taking the next steps to smarter public safety
- 15 Conclusion
- 16 For more information

## Executive Summary

Preventing crime. Anticipating and averting terrorist threats. Responding in real time to disasters and emergencies. These are some of the most pressing challenges facing today's city leaders. And they are the expectations of an increasingly demanding and digitally savvy public. Public safety greatly influences where people choose to live, work and play, and where businesses choose to locate their operations. And advances in technology are changing the way they think about public safety. The opportunities afforded by technology are demanding new ways of working and enabling cities to mount a more sophisticated defense against an ever-evolving threat landscape. They are also forcing a paradigm shift in how citizens expect municipal leaders and public agencies to act in the face of such threats.

New approaches focus on automating the capture and analysis of information from all kinds of business processes and devices, then applying the intelligence to help cities proactively recognize events and coordinate responses in real time. They are enabling cities to break down the communications barriers that often exist between first responders, jurisdictions and supporting agencies like public works, weather and transportation. Thoughtfully employed, these technologies are transforming public safety and the cities that implement them. They are positioning those cities to address unpredictability and risk and to improve quality of life for citizens. Today, cities around the world are actively using technologies to:

- Automatically alert first responders of malicious activities, events or actions that impact citizens' safety
- Conduct forensic searches for specific objects, colors, activities and human attributes across millions of indexed video clips and retrieve results in seconds and minutes
- Proactively predict events and vulnerabilities based on vast amounts of information captured and analyzed
- Replace dozens of aging, fragmented security systems with integrated solutions that strengthen protection while substantially mitigating the rising cost and complexity of security
- Control access to information and applications dynamically using rules-based identity management
- Make critical business data available to all users, irrespective of their location, to enable continuous delivery of vital services to citizens, even in the event of an outage
- Provide decision makers with a real-time, holistic view of the city's operations and resources, helping public agencies coordinate emergency response efforts and marshal resources in minutes and hours instead of days.

This is the essence of smarter public safety. Empowering organizations with the insights and intelligence to address—and prevent—potentially harmful events with speed and efficiency.

This paper looks at these and other examples of smarter public safety, not just to illustrate what the latest technologies make possible, but to explain how IBM is helping cities use these technologies to achieve results quickly while making transformational improvements in public safety.



## Introduction

The growing complexity and rise of diverse, unpredictable threats and natural disaster are changing the security landscape and rewriting the rules for public safety. Against a backdrop of shrinking budgets and resources, new technologies like cloud computing are enabling city leaders to strike back, changing the way they approach security and public safety, and arming even small cities with tools to manage threats with speed and efficiency—and do it cost-effectively. Rather than investigate events after the fact, smarter public safety shifts the focus to prevention, helping cities implement the strategies and tactics to anticipate and prevent attacks before they materialize.

Cities that have made the transition are employing analytics to build their intelligence and assess threat potential proactively. They are automating video search and analysis, establishing rules for the detection of unusual activities and the tripwires for notification of first responders. They are anticipating the kinds of risks that might inhibit continuous operations when an unforeseen event occurs. They are sharing security information across agencies, improving operational effectiveness and allowing for a coordinated, citywide response to incidents.

The cities profiled in this paper have made these changes. They have supplanted the traditional reactive approach to public safety. Instead of implementing safeguards after the damage is done, they are actively preempting and diffusing threats—and they are seeing the results (see table). And while it's hard to quantify the exact financial benefits of threat avoidance, these cities are making immediate and measurable gains from reduced crime and more rapid response to emergencies.

---

### Smarter Public Safety Results

---

Criminal acts across a European public rail network are detected dynamically and investigated rapidly using advanced video event correlation and analysis. Investigators can search through millions of recorded events and identify perpetrators in minutes, speeding apprehension and averting future crime.

---

Two U.S. cities are now able to issue citywide alerts and coordinate their response to threats and emergencies via a centralized command and operations center capable of consolidating security intelligence and feeds from cameras, sensors and other sources.

---

A U.S. state decreased the cost of its security operations by as much as 30 percent while significantly increasing system uptime and availability by outsourcing its security operations and implementing a fully integrated suite of security assessment, monitoring and management services.

---

A European city reduced its time frame for new employee activation by 100 percent—enabling same-day productivity—by automating identity management and establishing policies to control access to critical data.

---

A city agency achieved 40 percent savings by implementing a cloud-based disaster recovery solution for critical information and services, which automates backup and provides recovered files in hours, instead of days.

---

In less than one year, a major Brazilian city accelerated its crisis response to annual storms and flooding by integrating information and processes for more than 20 different city agencies in a single intelligent operations center.

---

### Protecting public rail and other transportation systems

Few issues are as important to urban professionals as public transportation<sup>1</sup>. Dependence on these systems for safe, reliable transit is growing, especially as gas prices continue to surge. But a city's transportation systems also have major implications for businesses and city leaders focused on commerce, development and the environment. A major disruption in operations can have a debilitating effect on the local economy, not to mention public trust.

Like most mass transit systems, this European country's sprawling nationwide rail network and numerous access points made it an easy target for criminal activity. Onsite security guards could only monitor what their eyes could see, leaving many railway assets (tunnels, power and substations, bridges and railyards) exposed. Video cameras were capturing events but not enabling them to be dealt with until after the crime had been committed. As a result, significant time and money were being spent to repair and recover rail system assets that had been vandalized or stolen. This prompted the rail provider to implement IBM's smart surveillance solution, Video Correlation and Analysis Suite (VCAS), across its rail network.

Today, at nearly 150 critical sites along its railways, millions of events are recorded in real time by digital cameras and sensors, then indexed and analyzed using vision and pattern recognition software. Alerts are triggered automatically when events defined by the rail provider occur, such as when luggage is abandoned on the platform or people loiter for extended periods. The solution delivers quick results: within seconds, onsite security guards are directly notified on monitors at their control center.



Alerts are also triggered if a certain sequence of events occurs, for example, if a person on the platform dwells on or beyond the yellow line for more than the specified amount of time. This ability to pre-define the objects, activities or scenarios that trigger alerts enables the rail provider's security forces to concentrate exclusively on incidents that require their intervention or decision making. Instead of laboriously viewing every bit of video captured, they can spend their time attending to developing situations that truly warrant their attention.

But captured video is only part of the story. What makes this surveillance system so powerful is its ability to integrate the output from multivendor sensors, detectors and event analysis systems and algorithms. Solution deployment was simplified by the open architecture of IBM's surveillance system, which facilitated integration with the rail provider's existing surveillance infrastructure and its diverse collection of analog and digital cameras. This lowered the provider's capital outlay and accelerated return.

Furthermore, the rail provider is able to avoid the costs and delays associated with manual, around-the-clock inspections of station platforms and rail cars before they leave the yard. Graffiti and other uncontrolled activities have lessened considerably in areas where the solution has been implemented. Not surprisingly, the provider's ability to better manage risk has resulted in higher customer satisfaction and ridership.

---

### What is smart surveillance?

More and more cities already challenged by resource constraints are finding it necessary to monitor public areas to keep them safe and accessible. Unlike traditional video surveillance solutions, which put the onus on people to sift through volumes of captured content, smart surveillance solutions leverage intelligence, automation and analytics to proactively prevent, and swiftly detect and react to suspicious events.

IBM's smart surveillance solution, Video and Correlation Analysis Suite, analyzes captured video as events happen, in real time. It dynamically integrates and correlates events from all kinds of cameras, sensors and detection systems, and sends alerts when established safety thresholds are exceeded. Video sequences are continuously analyzed with location-based situational awareness to intelligently monitor the movement and activities of people and objects against established norms and patterns.

All activities are indexed, enabling operators to initiate specialized searches for specific events, combining search criteria, like time, area, clothing or object color, and personal characteristics. The ability to retrieve results in a matter of seconds revolutionizes the investigative process, exposing perpetrators and threats before damages escalate.

---

In addition to these capabilities, IBM can help rail providers and city agencies to go beyond monitoring the scene. Data generated by biometric devices, license plate and facial recognition systems, fire and smoke detectors, motion detectors and onsite ATMs can be analyzed. By cross-indexing and correlating all of this information in a single repository, a rail provider can develop a more complete and accurate picture of suspicious events. This provides the ability to manage the data generated, perform forensic event-based retrieval and identify long-term statistical patterns of activity. Operators can submit a wide range of queries to locate objects of a certain type, color and size at a particular time. Indexed metadata generated for each recorded event simplifies and accelerates the search across the millions of events catalogued by the system daily. This allows security forces to attain key insights about troubling events in a matter of seconds and minutes, and act quickly to prevent any further disturbances.

## Defending city streets against criminal and terrorist acts

Following 9/11, cities across the U.S. were forced to examine their own preparedness for a terrorist attack and ensuing crisis situation. Most stepped up public safety measures, increasing public awareness and their capacity to react swiftly in the event of an attack. Many recognized that a major weakness of 9/11 was the lack of coordination of resources and response among all of the agencies trying to help. Two cities that saw it as a critical variable in the success of their own counterterrorism and public safety measures made the decision to implement a citywide surveillance network that could dramatically improve their ability to detect, prevent and respond to threats.

In both cases, IBM helped city engineers design and deploy an innovative surveillance strategy and infrastructure to capture, monitor and fully index video for real-time and forensic public safety applications. Each city erected a unified fiber network to provide base coverage of the most densely populated downtown areas, supplemented by an extensive wireless infrastructure to provide additional coverage, where required. Hundreds of new surveillance cameras were installed on the networks, and existing cameras were linked. Today, thousands of cameras in each city cover landmarks, venues, intersections, walkways and waterways, and all of their output is fed to a single, centralized command and operations center.

As with the European rail network, public as well as private cameras capture and store video that can be used in criminal investigations. But for these cities, the command center is the security intelligence hub and coordination point for emergency response. It is where algorithm-driven visual analysis identifies potential incidents and automatically notifies authorities. The command center also has the ability to process and



IBM Smart Vision Suite: Real-time video indexing and data analysis

analyze video feeds from the private sector. The feeds are then consolidated with feeds from publicly owned cameras and sensors. Instead of asking questions about what others are seeing at the scene, command center operators can see exactly what local operators are seeing. They can receive alerts and query information on hundreds of millions of events. They can also have eyes on the scene when the 911 calls come in from citizens. As soon as the caller's location is identified—usually in seconds—real-time feeds from the area can be viewed in the command center and then shared with the city's network of first responders, ensuring a highly coordinated response to threats. Such collaboration is essential to resolving issues efficiently and reducing the impact of crisis situations.

The command center's dashboard allows real-time notifications to be relayed to first responders instantly through a web portal, emails and handheld devices. The center's ability to see deep and wide enables dispatchers to identify dangerous situations for police and other responders, improving their safety. At any point in time, command center dispatchers can determine what resources are available, where they are located and how best to apply them. This real-time, integrated view of city emergencies and resources enables officials to direct the most appropriate response to each situation, while preserving critical services and resources. These cities can marshal resources in minutes and hours, instead of days, to warn citizens and provide targeted assistance. Furthermore, investigators who used to spend most of their time chasing down information can now locate what they are looking for in a matter of seconds, allowing them to perform investigations faster and, in many cases, prevent criminal behavior from developing. Likewise, first responders are able to react more rapidly. They are more likely to get to the scene in time to avert violence and victimization, potentially saving lives.

Other municipal agencies have also benefited. Smart video surveillance is enabling city transportation officials to monitor daily traffic patterns, alert citizens to bottlenecks and improve traffic flow. Public works officials are able to monitor city-owned vehicles, equipment and the illegal dumping of garbage and debris.



As the population of these cities has grown, so have their public safety networks. Built to scale easily, the networks enable new cameras to be easily integrated. IBM's unique wireless solutions allow the cities to deploy large numbers of additional cameras at the exact locations required, but also transport real-time video wirelessly, saving city taxpayers the cost of building out the wired infrastructure (estimated to be in the millions). Equipping first responders with mobile network access has also reduced dependence on the wired infrastructure. The ability to connect from their vehicles increases their effectiveness, speeding response while helping to control infrastructure costs.

---

*Investigators who used to spend most of their time chasing down information can now locate what they are looking for in a matter of seconds.*

---

The results achieved on city streets are being extended to city facilities. IBM is helping cities implement public safety solutions to protect the critical infrastructure of their school systems, roadways, power distribution centers and financial centers. And the implementations can accommodate accelerated time frames. Dedicated surveillance systems and the supporting network infrastructure can be up and running in days, not months.

### **Lowering security costs while strengthening protection**

The rising cost of security is an issue for all levels of government, especially as malicious attacks of public networks increase and become more expensive to resolve. The financial toll of a breach over and above defense and settlement expenses can be exorbitant, as agencies must factor in the cost of controlling damages and covering the losses of affected parties.

For one U.S. state governor, escalating security costs were compounded by the very real fear that current security systems were unable to protect the state's resources. Motivated by the state's vulnerability to attack and frustrated by attempts to address current operational inefficiencies in-house, the governor made the bold decision to outsource the state's

security infrastructure. The goal: to deliver far better protection while reducing costs to taxpayers. Realizing that security was not a core competency, state leaders agreed that they were putting citizens and resources at risk by continuing to manage security internally.

At a fundamental level, the state needed to consolidate its security infrastructure, eliminate redundancies, allocate resources more efficiently, and implement best practices statewide, across all of its agencies. To keep costs down, the state was not looking to remediate all potential vulnerabilities. Rather, it aimed to prioritize spending on active threats that would have the greatest impact to its operations. So implementing services that would help state leaders manage risk was key.

Working with IBM, the state's technology organization implemented a full suite of security assessment and management services to identify and address weaknesses and provide in-depth monitoring to reduce vulnerabilities and prevent breaches on an ongoing basis. The deployment was completed in about six months.

IBM's Managed Security Services centered on protecting the state's network and systems. They include firewall management, intrusion detection and prevention, vulnerability management and security event log management. They provide protection from both known and unknown threats via continuous security monitoring and immediate response when potentially damaging incidents are uncovered internally on the state's network perimeter. Their ability to aggressively eliminate malicious traffic helps optimize the state's uptime and availability.



The managed services also lowered the state's security-related operational costs, which were spiraling out of control, due in large part to individual agencies' complex array of aging, multivendor security systems. These systems had become complex and difficult to manage, and hiring and training employees to maintain and troubleshoot the fragmented assortment of applications and devices was costly. The decision to replace those systems with an integrated security solution enabled the state to significantly lower its operational costs—by as much as 30 percent. This was facilitated by visibility from a single management console, which provided the state's security operations with a consolidated view of the entire security infrastructure. In turn, the state was able to reallocate many of its operational resources to a more strategic role.

The state's decision to comply with the Federal Information Security Management Act (FISMA) helped to bolster its IT budget, but also to improve constituents' perception of its security protections. IBM's FISMA gap analysis enabled the state to evaluate its security posture against the FISMA standards, identify and remediate inconsistencies, and build a compliant environment with the mandated management reporting and operational and technical controls.

Today, state leaders continue to make great strides in protecting the state's financial assets and intellectual property, while boosting its reputation for citizen safety and security. The task is made easier through the use of IBM's advanced analytics, which are helping the state identify new exposures continuously. To further reduce its risk of data breaches and avoid compliance failures, state leaders are considering IBM's

security information and event management system. The system can enhance the value of the state's current security systems by providing proactive threat detection with behavioral and heuristic-based detection techniques.



### **Securing confidential systems and information from unauthorized access**

Following decades as a coal mining center, the small city of Karviná in the Czech Republic has emerged a major commercial, cultural and tourist hub in Central Europe. Modernization of the city, along with the explosive growth of data, devices and connectivity, has made information security increasingly difficult and complex for Karviná to manage.

As with other growing cities, threats to Karviná's systems and information became more sophisticated and relentless, and addressing potential security breaches was becoming more costly. At the same time, Karviná's small size limited its IT resources. The city's manual processes for provisioning and monitoring access to systems, implementing controls and enforcing them were overwhelming its IT personnel. The processes also created serious security risks because they were prone to error and because manual processing enabled terminated employees to retain access for several days. City leaders wanted a simpler, more cost-effective means of protecting their vital systems and information from unauthorized access, without soaking up precious resources.

Karviná implemented IBM's Identity and Access Management (IAM) solution to centralize and automate its time-consuming access control processes, simplify administration and monitoring, and prevent unauthorized access to the city's systems and information. Its rules-based identity management system enables Karviná to control employees' access to critical data and applications based on their position, role and department. Administrators set and enforce policies for who has access to what information, when they can access it, and from what devices and locations.

---

*Today, new employees become productive, with access to all systems, in a few hours, compared with several days previously.*

---

Since employees' roles and responsibilities are constantly changing, Karviná can use the system to review, reconfirm or update employees' privileges, or promptly revoke them

when necessary. The system uses an automatic account reconciliation process to continuously detect and correct (or remove) any employee accounts that are not in agreement with predefined rules. Orphan accounts are automatically removed and employee accounts are deactivated within hours of an employee's termination. This allows Karviná to proactively protect against policy violations while ensuring the security of its sensitive data and applications.

The Identity and Access Management solution has had a dramatic impact on Karviná's administrative efficiency and has lowered its costs. The city has seen a 100 percent improvement in the speed of new employee activations. Today, new employees become productive, with access to all systems, in a few hours, compared with several days previously. Perhaps, more important, access management for all of Karviná's user accounts can be handled by a single IT administrator, lowering costs while enabling the rest of the IT staff to focus on strategic improvements that have citywide reach.

### **Maintaining access to critical information and services when disaster strikes**

Continuity planning and recovery are cornerstones of a city's resilience and long-term vitality. Disaster readiness reduces the disruption to city operations and productivity, and it enables public agencies and other support organizations to play a stabilizing role in the community. Service continuity is especially critical during disasters. It ensures that basic human services are provided to those who are most in need.

For one human services agency in the U.S., that means bringing education, employment programs and social services to more than 200,000 people in its home city and surrounding regions. Along with a wide range of programs to improve the quality of life for children, seniors and families in the city's vulnerable neighborhoods, the agency leverages its network of

resources to deliver “people-centered recovery efforts” during disasters. Ironically, the agency’s systems were not designed for disaster situations, lacking the necessary speed and efficiency.

---

### **What is cloud computing?**

**Cloud computing is an approach for rapidly delivering IT services and applications via the Internet utilizing a flexible pricing model.**

**The cloud enables cities to lower the cost of IT by alleviating the need to make capital investments in hardware and software, or pay for idle computing resources. Instead, costs are based on usage, so you pay only for the resources used.**

**Cloud computing also goes beyond cost savings by allowing users to access the latest applications and capabilities in support of your services.**

---

After two destructive hurricanes struck the area, the agency was called into action. So, too, were its backup and recovery systems, which were ill-equipped for a disaster. As agency personnel worked to connect the people living in the city with the services they needed, then assist thousands of evacuees from other affected cities, the systems’ inefficiencies became crystal clear. Faced with requests to provide both emergency and continuing care, including employment, housing and health services, the need to record and store information in support of all of the affected individuals put a massive strain on the existing systems.

The agency lacked sufficient redundancy for its data backup and recovery systems. Tape backups were handled manually at headquarters, with a third party handling offsite vaulting. Administrative staff at the agency’s seven locations and 60

remote sites were responsible for storing their own backups. With all of the agency’s offsite storage situated locally, recovery could easily be compromised. Further, with 500 gigabytes of data growing at an annual rate of 40 percent and the need to retain daily, weekly and monthly backups to meet business requirements, the agency’s storage needs and costs were escalating rapidly, along with concerns about meeting strict compliance requirements.

Agency leaders chose a cloud-based managed backup and recovery solution to reduce their operational risk and allow implementation in six months or less. IBM SmartCloud Managed Backup enabled the agency to replace its manual, do-it-yourself approach with daily, automated incremental backups of its business and client data, as well as communications from its email servers and individual user mailboxes, at all agency locations. The cloud solution also offered an important financial benefit. With all of the hardware, software and support services provided by IBM, the nonprofit agency didn’t have to worry about any additional capital expenditures or upfront costs.

The automated system simplified the agency’s backup and restore processing. Using a customized web portal, administrators could update backup and restore settings and criteria, initiate service and monitor all data backup and recovery activity. As data volumes changed, the solution adjusted automatically to meet the new backup requirements. As a result, the number of IT resources needed to oversee backup and recovery dropped significantly, and the agency was able to redirect personnel to more pressing IT challenges. The automated system also provided rapid access to information; users could view backup files and recovered data in hours instead of days. In addition, the agency was confident that it would be able to meet all relevant compliance requirements for data backup and retention.

While the agency's primary data center facilities remained at headquarters, a redundant site was established 1,200 miles away at an IBM Business Continuity and Recovery Center. The redundant site enables agency staff to access critical business data at all times, even in the event of an outage. Auto-generated event and summary reports, configured to the agency's needs, monitor backup completions and track failure patterns. With better insight into service usage and historical trends, the agency has been able to lower its risk. Plus, the solution's scalable managed protection and pay-as-you-go pricing have enabled the agency to control storage costs while better managing its regulatory compliance requirements. IBM has been able to reduce total cost of ownership for clients by as much as 40 percent while improving service levels.

---

#### **Why choose cloud-based data protection services?**

Cloud-based data protection solutions reduce capital outlay, limiting the need for hardware expenditures. There is no need to keep adding disks and drives or to deploy a redundant and dedicated physical infrastructure. Users can easily switch from a capital expense model to a monthly operating expense model, often with considerable savings.

Data storage is scalable and elastic in the cloud. As storage needs increase, a cloud-based backup service can scale easily to accommodate the difference. The cloud's systematic and automatic backups also increase availability and enable faster recovery when disruptions occur. Data can be restored instantly regardless of a user's location or time zone.

---

#### **Protecting citizens with faster and more coordinated crisis response**

Preventing the impact of disasters was already a significant concern for Rio de Janeiro when a series of flash floods and landslides claimed lives and caused widespread infrastructure damage in 2010. The torrential summer storms were not uncommon, but their effects could have been diminished if Rio had a single, central location capable of monitoring the unfolding disasters and overseeing the response. With the 2014 World Cup and 2016 Summer Olympics on the horizon, it also raised serious questions about Rio's emergency preparedness and pointed to the dire need for better communication between the people and systems that served the city.

If Rio's meteorologists, engineers, field operations and crisis response personnel had worked together, would citizens have been better prepared for the disaster? If the operational silos that separated these organizations were eliminated and their systems were able to share information in real time, would it have been possible to proactively determine where flooding and landslides were most likely to occur, where shelters and hospital beds would most likely be needed, and which evacuation routes would be the safest? If such communications were possible, would Rio's response have been swifter and more effective?

Such questions prompted Rio's city leaders to collaborate with IBM on the development of a solution to integrate the city's core operations to enable real-time communications and a more proactive approach to crisis management. Rio's

intelligent operations center was up and running 16 weeks later, and in less than one year, the center was integrating information and processes from over 20 different city agencies—municipal and state departments as well as private utility and transportation companies. This provided officials with a holistic view of city operations at any point in time, allowing them to handle emergencies with all hands on deck.



Rio intelligent operations center<sup>2</sup>

Today representatives from each agency actually sit side by side in the operations center and look at live feeds of city streets and facilities. They are collaborating to assess and respond to threats, but also to manage the flow of traffic and public transportation systems, and monitor the efficiency of power and water supplies. They have the ability to work together to mobilize response teams, prepare shelters and deploy needed equipment and supplies, as situations warrant. They are actively sharing information and making group decisions dynamically.

The operations center relies on a system that uses situational awareness and predictive analytics to sense and coordinate response to emergencies. The system's high-resolution weather forecasting capability, for example, uses a global weather model and algorithms to predict heavy rains. The system pulls data from Rio's river basin, topographic surveys, historical rainfall logs and radar feeds, helping operators calculate the effects on traffic, power and other city services. When urgent situations are detected, like changes in the flood forecast, an automated alert system notifies city officials and emergency personnel via email and instant messaging. Working alongside Rio's own radar and the satellite from Aeronautics, the system allows more time for Rio's officials to prepare for storms and prevent disaster.

Operators are able to monitor dozens of real-time data feeds, which provide them with the insights to anticipate looming problems and help city leaders put defenses in place to lessen their impact. Not only is the city better able to handle emergencies, city leaders can use the same tools to prepare Rio for major events like public concerts, parades and sporting events. In addition, first responders are using the wealth of information collected to tweak their system settings and operational procedures to speed response and better coordinate their efforts on citizens' behalf.

*When urgent situations are detected, like changes in the flood forecast, an automated alert system notifies city officials and emergency personnel via email and instant messaging.*

In January 2012, Rio's ability to respond was tested when three downtown office buildings collapsed. Almost immediately, the operations center notified fire and civil defense departments and contacted gas and electric companies to shut down service around the scene. Rapid notifications also went out to close the subway underneath the site, block streets, dispatch ambulances, alert local hospitals and send in heavy equipment to remove the rubble.

---

#### **Why establish an intelligent operations center?**

**Most agencies capture enormous amounts of data. Intelligent operations centers (IOC) provide the means to share that information across organizational and jurisdictional boundaries.**

**Though IOCs serve as central coordination points for information, they need not be in one physical location. The important thing is that they provide access for all city domains, from first responders to transportation, building and energy management, health and education.**

**Cities can deploy a dedicated IOC at a designated facility or leverage a shared IOC at an IBM data center or on the cloud.**

---

Over and above the public safety benefit, the system provides Rio's citizens with access to information that improves the way they live and work. The same weather and traffic information used by city administrators is shared with citizens on mobile devices and social networks. When the buildings

collapsed, citizens were alerted via Twitter, Facebook and other social media. On any given day, the operations center issues notifications about traffic accidents, street closings and any other events that are likely to impact citizens' daily routine. This empowers citizens to make choices that minimize personal inconvenience but also improve the overall flow of city operations. The result is a city that is more attractive to residents, tourists and business investors alike.

#### **Taking the steps to smarter public safety**

Cities are increasingly looking for ways to anticipate, prevent and respond to threats. But developing a cost-effective roadmap for smarter public safety—one that can assimilate massive quantities of information and provide decision makers with a comprehensive, real-time view of city operations—can extend beyond a city's own capabilities.

IBM has extensive experience helping city, state and national agencies leverage technology to protect citizens. Our technologies and services are enabling them to integrate and automate their security operations, transform stores of collected information into intelligence, protect against cyber threats, and provide the advanced analytics to streamline disaster preparation and response. It is the foundation of smarter public safety and the basis of our service offerings.

Applying the best practices identified from working with municipal IT departments and decision makers, we have developed a suite of services and technologies that can be customized to align with each city's unique budgetary and functional requirements. We offer an array of resources to help cities and agencies address their public safety needs.

One place to begin is our [Smarter Public Safety portal](#) to learn more about our physical security solutions, connect with our experts and download additional case studies. Talk to your IBM representative about how we can perform an assessment of your physical security environment to better understand your current controls and processes, and develop a strategy for improving them.

Our [Smarter Security and Resilience portal](#) explains how it's possible to change your security approach from "experience and react" to "anticipate and adjust." Our [Business Continuity Index](#) tool can provide you with an accurate picture of your stance on risk and resilience, along with recommendations for improvement. And our complimentary [Security Health Scan](#) analyzes your network to determine vulnerabilities and provides recommendations on how to remediate threats. These are just a few of the tools that provide insights you can leverage on your path to smarter public safety.

Our technology professionals will help assess your environment and customize and implement a smarter public safety strategy capable of delivering tangible value, including cost-effective service delivery, reduced complexity and higher availability. Our disciplined approach, based on decades of IT service experience, is designed to deliver measured business outcomes and exceptional value for our clients. Today, it is enabling IBM to help cities of every size and geography to better meet the safety and security needs of their citizens. And we can do the same for your city.

## Conclusion

Every day, cities around the world face an increasing barrage of threats from a widening array of unpredictable sources. As enablers of progress and development, city leaders will continue to take center stage in the decision to implement smarter public safety. By focusing on public safety initiatives that take advantage of new technologies, analytics-driven intelligence and automation, cities can overcome the challenges that impede their ability to predict threats and take preventive actions today. City leaders who can integrate siloed systems and fragmented city operations, share information across state and municipal departments, and deliver a coordinated, real-time response to emergencies are not only better prepared to address the expanding scope and impact of threats, they strengthen their ability to govern effectively. They are not only better able to assure citizens' safety, they are better equipped to build a safe environment for growth and commerce.

However, rapid payback will be critical for public safety initiatives, especially with limited funding available for such improvements. With cloud's low cost of entry and potential to significantly reduce public safety and security expenses, it holds considerable promise for today's budget-constrained cities. City leaders who can use this and other IT solutions to demonstrate results quickly will make the greatest gains financially and operationally.

Armed with the advanced tools and processes to deliver meaningful intelligence and enable seamless collaboration among public agencies and first responders, cities can begin to proactively address threats and speed rescue and response. They take a major step forward in improving citizens' safety and providing the quality of life needed to drive business development and economic growth.

## For more information

To learn more about how IBM is helping cities implement smarter public safety, please contact your IBM representative or IBM Business Partner, or visit

[ibm.com/smartercities](http://ibm.com/smartercities)



---

© COPYRIGHT IBM CORPORATION 2012  
IBM Global Services  
Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America  
November 2012

IBM, the IBM logo and [ibm.com](http://ibm.com) are trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or TM), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. Other product, company or service names may be trademarks or service marks of others. A current list of IBM trademarks is available on the web at “[Copyright and trademark information](http://ibm.com/legal/copytrade.shtml)” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Actual available storage capacity may be reported for both uncompressed and compressed data and will vary and may be less than stated.

<sup>1</sup> “[Livable Cities: Challenges and opportunities for policymakers](#)”  
Economist Intelligence Unit, November 2010.

<sup>2</sup> Photo courtesy of Raphael Lima

