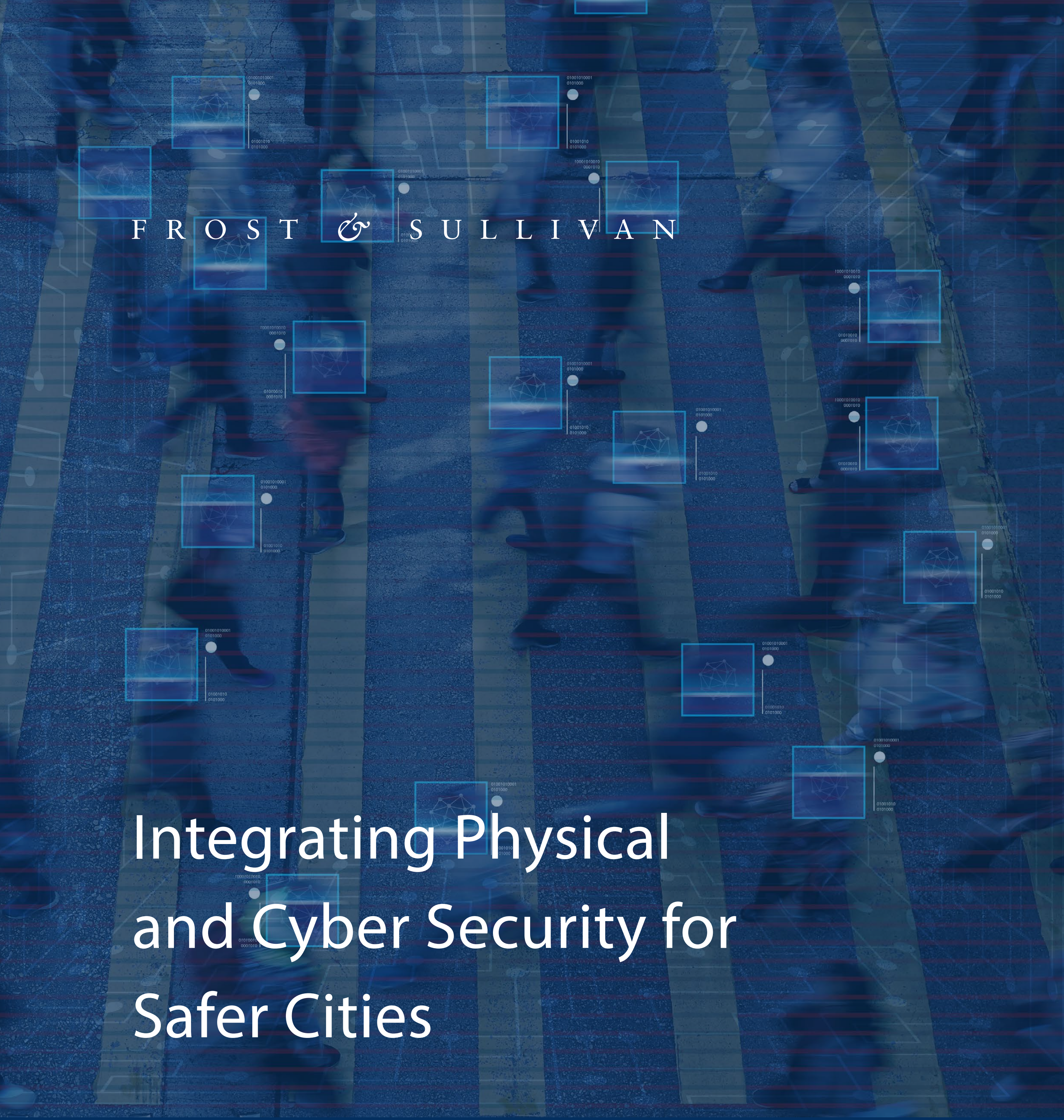


FROST & SULLIVAN

Integrating Physical and Cyber Security for Safer Cities

A Frost & Sullivan White Paper
Commissioned by NEC

\Orchestrating a brighter world

NEC

WWW.FROST.COM

We Accelerate Growth

Table of Contents

01

A Brave New World

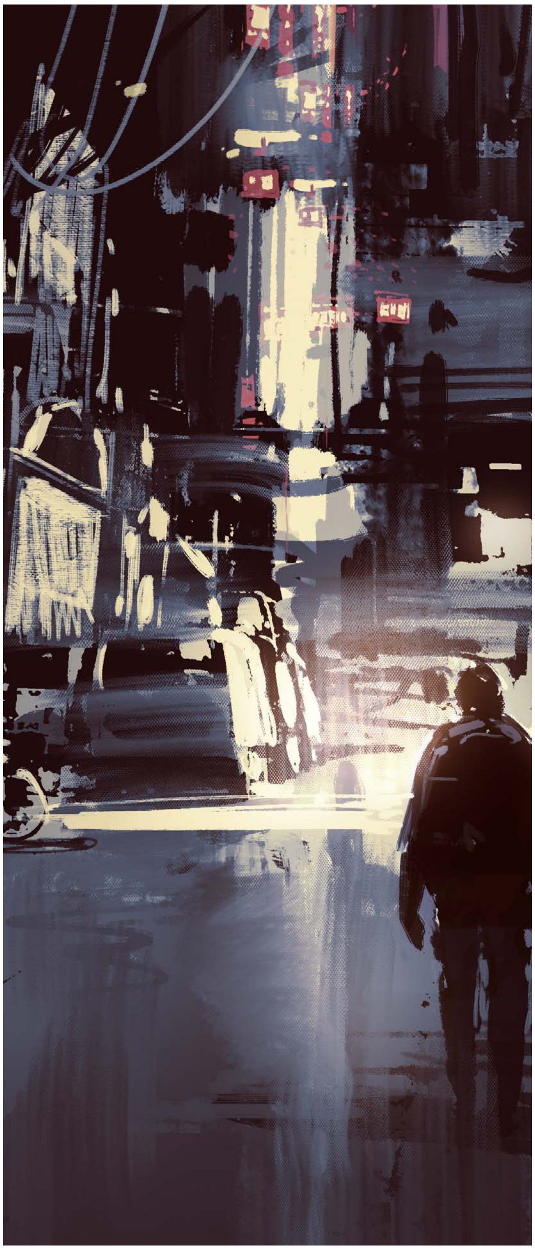
A DYSTOPIAN VIEW OF THE FUTURE

The implications of globalization are more prominent than ever. As people become more mobile, the mass movement of people into urban centres in search of opportunities create unprecedented challenges. Urban planners come under pressure to devise smarter ways to manage public safety, transportation, sanitation, and law enforcement. Cities compete with one another for resources and those that are effective in attracting and retaining talented people are more likely to succeed than those that are not. Corporations and government agencies are investing heavily in cutting-edge solutions and infrastructure development. While it is still too early to measure the full impact of technology on society, its pervasiveness continues to be felt.

While technological tools are key enablers to solving urban challenges, society does expect the government to ensure that their benefits outweigh the accompanying problems. When expectations fall short, people are inclined to express their frustrations through social media.

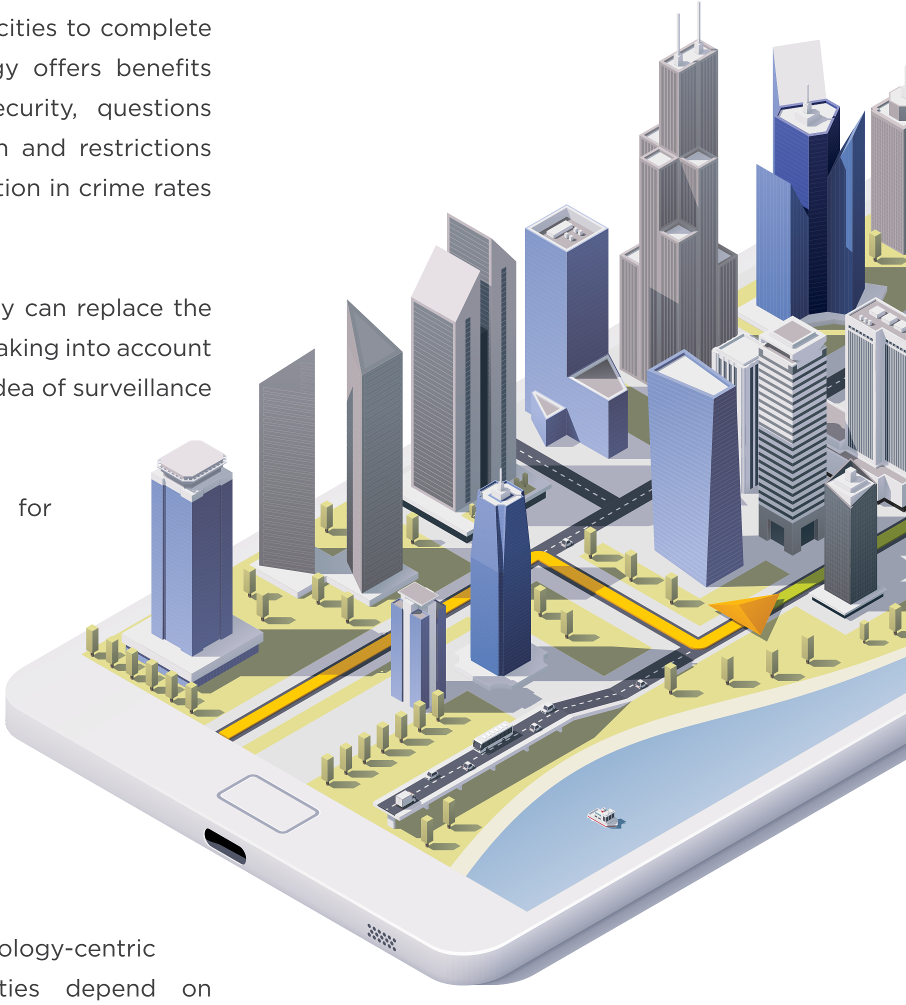
As governments address the various urban challenges facing cities using smart and safe city solutions, how will society look like in 2030?

In time to come, the proliferation of technology will address a number of urban problems we face today. One of the most significant improvements will be in public safety as public infrastructure is virtualized using embedded sensors, cameras, and wireless connectivity. As the pace of urbanization picks up, authorities are channeling more resources to modernize aging infrastructure. While this is beneficial, the costs involved and the sheer scale of dependence on them will make critical infrastructure vulnerable to cyber-attacks.



To safeguard critical infrastructure, authorities deploy smart city technologies to the point of subjecting cities to complete dependence on them. While the technology offers benefits in improving efficiencies, services and security, questions surrounding privacy, potential discrimination and restrictions to freedom do arise. Will a substantial reduction in crime rates make people feel safer?

Governments tend to believe that technology can replace the various aspects of law enforcement, without taking into account the growing unease among people with the idea of surveillance cameras and sensors in public areas.



Technology is improving efficiencies for corporations and government agencies by automating more labor-intensive processes, gradually taking away jobs from people. The resulting impact of unemployment could be worsened by rising costs in transportation, housing, and healthcare. Digitizing public infrastructure could translate into higher costs for the community.

The problem started when an overly technology-centric approach is taken. Government authorities depend on technology and efficiency to improve the quality of life in cities. However, the impact of smart city programs may not always benefit the people. The irony is that countries that are at the forefront of technology are said to be no happier than those lagging behind technologically.

Ideally, technological tools should lead to inclusiveness where citizens are empowered with information and alternatives to choose. As urban planners begin to understand that technology alone cannot solve all urban problems, they are shifting toward holistic solutions that bring the community and stakeholders together onboard the ecosystem and sustain them.

02

Integrating Physical and Cyber Security Concerns

Fast population growth in the city are putting a strain on existing infrastructure, as many have not been designed to cope with the demands of urbanization. The onset of aging is also besetting these facilities. In response, urban planners are striving towards digitization to increase automation and responsiveness.

The Internet of Things (IoT) are making the world increasingly connected. Technology convergence is integrating the physical and digital worlds, achieving efficiency levels not previously possible. However, this convergence can also present new challenges to urban planners and corporations.

For decades, the air gap separating operational technology and information technology made internal systems resilient. Cyber security was hardly an issue. The conventional focus was on protecting critical assets from physical attacks via restricted access, monitoring, and safeguarding security around the premises. Nevertheless, critical infrastructure remain vulnerable to physical attacks until today. Public places are often the choice for physical attacks despite of heightened security.

	PHYSICAL VULNERABILITY	CYBER VULNERABILITY
AIRPORTS	Long queues waiting to go through rigorous security checks at airports make them highly attractive soft targets	Increase in automated self-service installations that allow check-ins, baggage drops, and ID scans with minimal human intervention present risks
POWER GENERATION	Transformers that are typically placed outdoors make substations and power lines vulnerable to physical attacks	Technological innovations such as connected devices present new access points for invading the electric grid
CITIZEN SAFETY	Individuals have limited capacity in controlling threats to physical safety in densely populated areas	Identifiable information of individuals can be exposed through the hacking of public infrastructure
GOVERNMENT SERVICES	Physical breaches and unauthorized facility access may lead to vandalism and theft of assets and/or disruption of services	Frequent target of cyber-attacks with occurrence expected to be on a rise due to political dissent
DISASTER MANAGEMENT	Lack of established practices in emerging market economies to ensure the security of people and physical assets during incidents	Ability to penetrate and disable critical infrastructure from a remote place undetected
STADIUMS AND BIG EVENT VENUES	Emotional and hostile behaviour of individual/s at the venues subject spectators to physical harm	Attacks on connected networks can disrupt operational systems and cause power outages

Legacy systems lack the capabilities to detect and report on operational problems. Connecting these systems to a network makes them even more vulnerable to intrusion from a remote location. The integration of operational technology and information technology exposes critical assets to a higher level of vulnerability which existing systems have not been designed to meet.

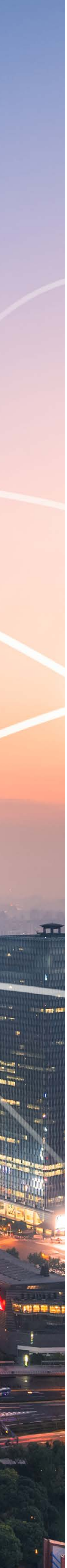
Long-established physical security practices often mislead security managers into believing that their networks are secure when in fact they are more vulnerable due to the lack of integration between their physical security and cyber security. Organizations are not taking sufficient measures to protect themselves. For example, in early 2017, a ransomware attack on the digital key system of a luxury hotel in Austria prevented 180 hotel guests from entering or leaving their rooms. The attack forced the Romantik Seehotel Jäegerwirt Hotel to accede to hackers' demands, by paying the ransom of €1,500 in Bitcoins (approximately $1.88 million).

Cyber-attacks are growing in scale and frequency at an alarming rate, reaching levels of sophistication that are difficult for authorities to trace. Holding an organization ransom can potentially lead to not only the disruption of operations and financial losses, but also physical harm. Attacks on transportation, water, telecommunication, energy, finance, government, and healthcare services have the capacity to destabilize an economy. While attackers may not have the skills, access rights or resources to destroy sophisticated equipment, a malware system hack can go undetected for some time and shut down the system until the financial demands are met. For example, a cyber-attack on Ukraine's power grid in the winter of 2015 left approximately 700,000 people without power for several hours. In 2016, Verizon reported an intrusion into its water treatment system where attackers altered settings related to water flow and the amount of chemicals for treating drinking water.

While security managers are familiar with the common types of cyber security attacks such as denial of service, malware, and phishing attacks, the rapid evolution of physical-cyber integration is likely to generate new vulnerabilities requiring decision-makers to have an in-depth understanding of future risks and to prepare for them. Cross-industry collaboration is essential in bringing together all relevant stakeholders. For example, the proliferation of electric cars can present new access points for invading the grid, making it necessary for power companies to work with automotive companies to strengthen their defense against physical-cyber threats. Organizations need to be a step ahead of cyber criminals. As they begin to mitigate physical and cyber security concerns, organizations can be better equipped to identify more "weak spots" by looking beyond their respective industries.

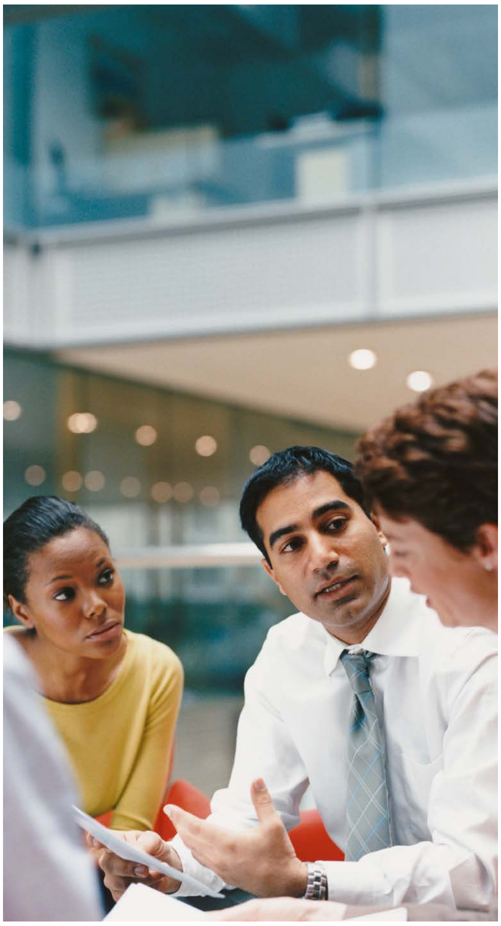
03

Key Applications Authorities Should Consider



Urban planners are juggling with multiple challenges to make cities better and more livable, as part of efforts to increase their competitive advantage. They are deploying more innovative ways of delivering public services. However, apart from enhancing operational efficiencies, urban planners are becoming mindful of the various threats that could negate their efforts. In the past, urban planners were most concerned about physical threats and natural disasters. Present technological innovations are introducing cyber threats that were not major concerns before. Thus, safety needs to be defined beyond physical threats.

There are numerous technological tools designed to produce safer outcomes. How can urban planners leverage horizontal technologies such as the IoT, big data, artificial intelligence, biometrics, and cyber security, and the integration of various emerging technologies? While there are numerous applications urban planners could consider, it is essential to prioritize resources by identifying the six most critical applications. They include border control, critical infrastructure protection, citizen safety, government services, natural disaster management, stadiums, and big events venues.



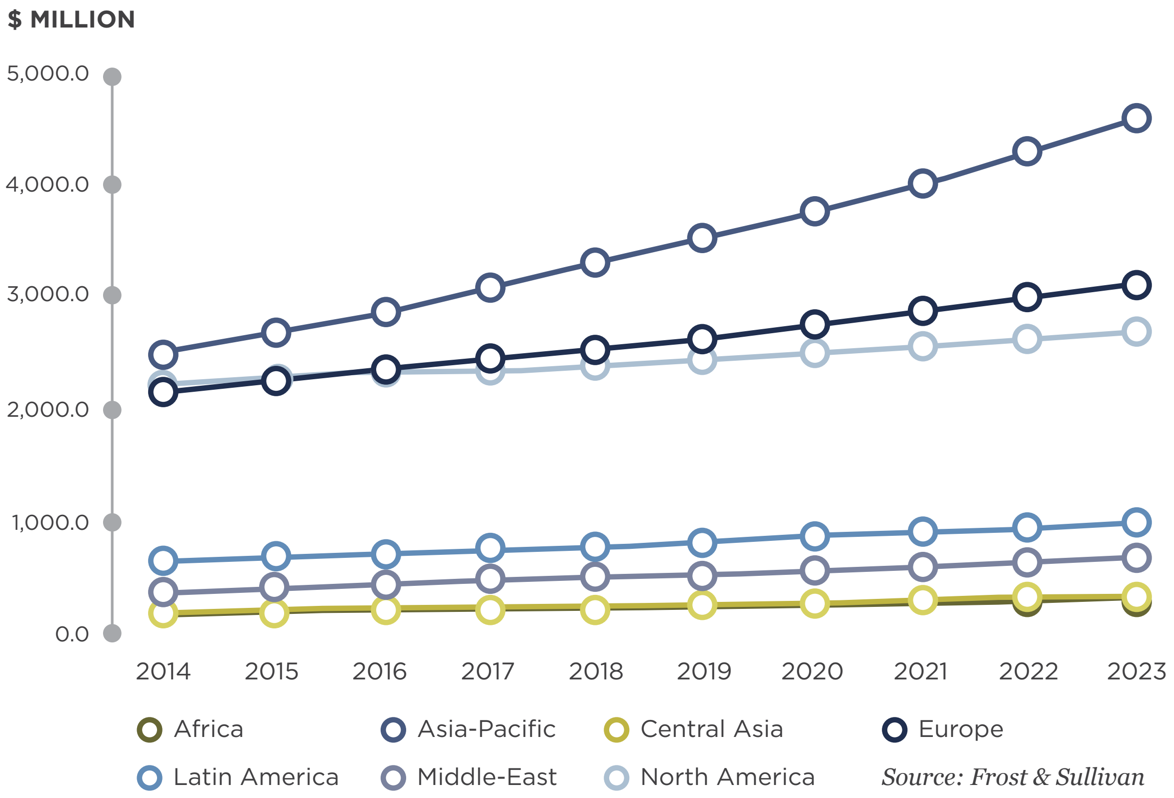
KEY APPLICATIONS	TYPES OF INNOVATIVE TECHNOLOGIES
BORDER CONTROL	With the increase in passenger traffic, preventing long queues at airport security checkpoints is a top priority. Multimode authentication for face, fingerprint, and iris recognition enables passengers to be verified at electronic gates with minimal human intervention while enhancing the flow of security checks. The deployment of high-resolution cameras, facial recognition algorithm, and advanced analytics that cross-reference to databases enable border control agencies to detect suspects and take immediate action before they leave the country.
CRITICAL INFRASTRUCTURE PROTECTION	Disruptions in critical infrastructure operations can bring about physical harm and potentially destabilize an economy. Surveillance capability can be enhanced with movement sensors, high-resolution cameras, and behavioural analytics that detect suspicious behaviour in restricted premises and control access using multimodal biometrics. Cyber security applications include a multi-layered defense for SCADA systems that detect abnormal behaviour with sensing, monitoring, and situational awareness while providing decision-makers with meaningful forensic insights to investigate security breaches.
CITIZEN SAFETY	The proliferation of innovative technologies in the form of wearables and mobile devices provide law enforcement officers with body cameras, handheld consoles for fingerprint reading, license plate readers, facial recognition technologies, and personal radar for detecting movements in places suspected of illegal activities. Over time, drones will be increasingly deployed for surveillance and monitoring especially in sparsely populated less accessible areas. Drawing data from several inter-agency databases, crime analytics provide insights on criminal patterns and predict when and where the next incident may occur.
GOVERNMENT SERVICES	Multiple users are accessing government services from their mobile devices, making agencies vulnerable to Internet threats. Capabilities to detect cyber security threats, information leaks, website manipulations, and machine learning enable systems to identify new cyber-attack patterns. Multimodal biometric solutions safeguard unauthorized access with video surveillance and alert options to support security personnel. Face recognition for surveillance using "facetraps" are gaining popularity with cameras installed in places (e.g., elevators, counters, TV monitors) where people are likely to look directly into a camera without realizing it.

KEY APPLICATIONS	TYPES OF INNOVATIVE TECHNOLOGIES
NATURAL DISASTER MANAGEMENT	While it is impossible to prevent the occurrence of natural disasters, urban planners seek a system that could, over time, show them and predict when and where a natural disaster is going to happen as well as the extent of the resulting impact. Sensors could be installed in risk-prone areas to collect data for analysis and scenario planning to enable rescuers to promptly identify the areas at risk and evacuate people before a disaster happens.
STADIUMS AND BIG EVENT VENUES	Public safety is a primary concern of law enforcement agencies during major events with global media coverage, while the smooth running of an event is the main priority of event organizers. Cyber-attacks that penetrate internal controls can bring down the operating system utilized by the event. Therefore integrating cyber and physical security is critical in protecting the network against ransomware attacks. Concurrently, the use of video analytics and advanced facial recognition is crucial in spotting rowdy and emotional sentiments that are characteristic of violent behaviour within large crowds in a stadium even when people are not directly facing a camera.

Ongoing concerns about government security infrastructure across many regions of the world are expected to drive the need for advancing border control systems. The global security market is estimated to be worth US$72.6 billion at the end of 2016. Increased priority in cyber security is transforming border control and biometric security into a fast-moving sector with well-developed policies, best practices, and legislation to support investment that will protect specific areas of the border.

At the same time, higher passenger volumes at airports and the accompanying risks as soft targets are increasingly demanding cutting-edge screening technologies to prevent long queues at customs checks. Long-term security investments are set to continue as airports seek to streamline systems and balance rigorous safety procedures with enhancing customer satisfaction levels using non-invasive security technology. Although airports traditionally focus on physical security, greater importance in cyber security investments can be expected with widespread connection of digital systems.

AIRPORT SECURITY MARKET: TOTAL EXPENDITURE, GLOBAL, 2014-2033

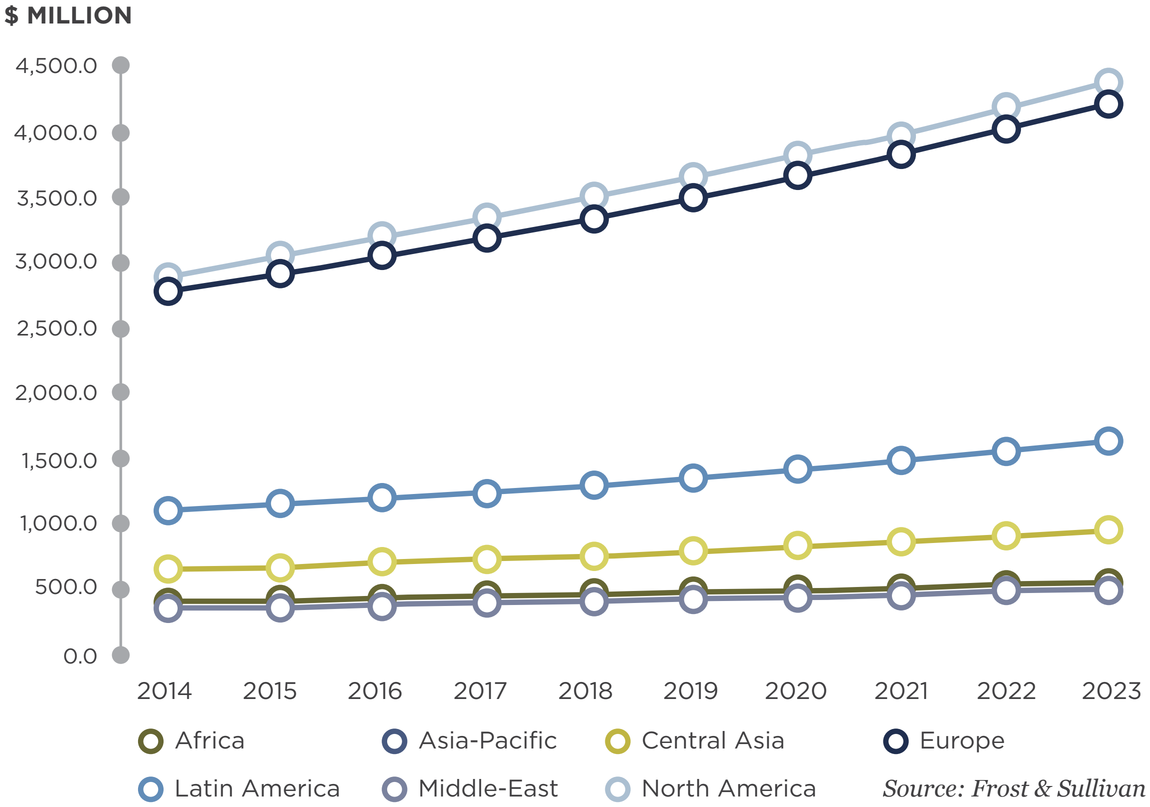


Source: Frost & Sullivan

Safety and security are major concerns for the utilities sector. Although physical security controls guarding restricted premises are well established, the growing use of connected systems demands the deployment of tighter cyber security measures. Utilities companies are coming to terms with the importance of building tighter cyber security measures into their automation processes. The provision of cyber security is coming on par with the overall physical security of the utility site including the emphasis on protecting remotely controlled operations.

While many biometric applications cater primarily to government needs, they are increasingly deployed in the private sector across several industries. The tourism sector is raising the level of customer experience with multimodal biometrics to provide access and authentication for entry into various facilities and enabling secure payments in hotels or resort premises. The use of facial recognition is particularly useful in casinos for spotting VIP guests and celebrities to provide preferential treatment, and identifying blacklisted guests who have been banned from entering the premises.

UTILITIES SECURITY MARKET: EXPENDITURE, GLOBAL, 2014-2023



Source: Frost & Sullivan

Facial recognition technology is also gaining traction in retail outlets for its anti-theft and customer behavior tracking features. High-resolution cameras and advanced analytics are deployed in luxury stores to match shoppers' faces to a database containing the photographs of past shoplifters. The technology is also being used to access customers' responses to displays and promotions, and to understand their behavior to devise more effective pricing and marketing strategies.

The automotive industry is looking toward biometrics to strengthen vehicle security. Replacing physical keys and fobs with more secure methods are under serious consideration, to address the ongoing vehicle theft and hijacking concerns. The adoption of multimodal biometrics provides a compelling point of differentiation for automotive makers. Besides allowing recognized people from entering and activating a car, iris detection tracks the alertness of drivers. In instances where a driver is falling asleep, the system will bring the vehicle safely to a halt.

Aggregated data on people in the streets, malls, and other public places can be extremely valuable information, for instance, to help authorities in tracking criminal suspects. Sharing of data among collaborative stakeholders can make a city a safer place for all.

With no direct interaction with people, biometrics is among the least invasive methods of assessing an individual. Nevertheless, people are aware that their movements are increasingly monitored, raising security and privacy concerns. People want to know how their information is being used. For biometrics to take off on a large scale, governments and organizations need to be more transparent in addressing these concerns.

04

Case Studies: Safer City Solutions

CASE STUDY 1

PUBLIC SAFETY WITH AN INTEGRATED IT SOLUTION

Tigre City, Argentina

Situated 32km northwest of Argentina's capital, Buenos Aires, Tigre is a city of 400,000 people. Since the 1990s, the city has been experiencing rapid population growth giving rise to the number of private neighborhoods. Tigre is also gaining popularity as a holiday destination among Argentines and overseas tourists.

Safety and security are top priorities for the local government of Tigre. NEC has been contracted to provide a holistic urban monitoring system to boost the safety and security of public places within the city. The solution comprises an advanced surveillance system with the installation of approximately 1,000 CCTV cameras at key public locations, intelligent video analysis, and a command-and-control center.

The system includes video monitoring, urban surveillance, advanced facial recognition, and behavior detection to help the police identify criminals, locate missing people, and spot suspicious behavior within a large crowd. A large amount of the data captured is processed in real time using NEC's image analysis technology to detect danger.

NEC also provides a wide variety of technologies to secure the road networks including real-time detection of human behavior associated with potential crimes such as speeding, double riding, and riding without helmets. The solution is also equipped with license plate recognition capabilities to locate stolen vehicles. Since the implementation of the NEC system, vehicle thefts in Tigre have dropped by 40%.

CASE STUDY 2

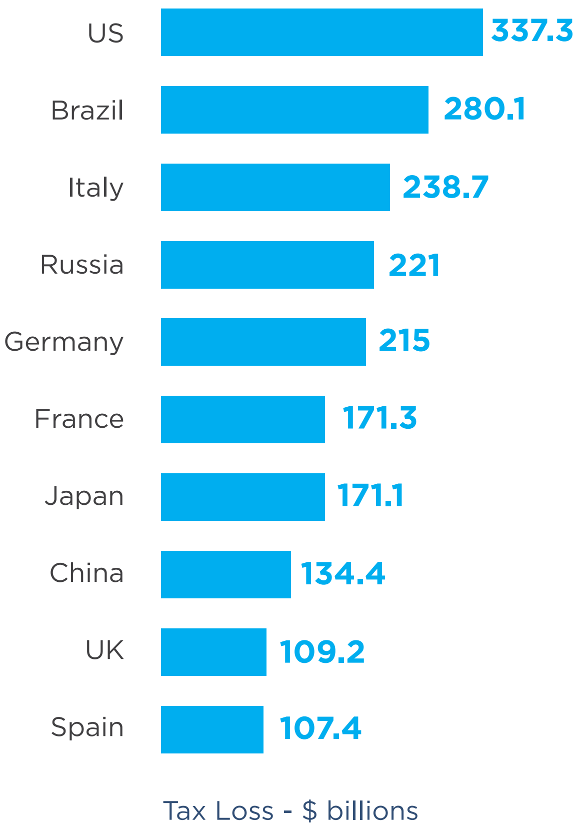
TACKLING TAX EVASION WITH FACIAL RECOGNITION

Brazil

Tax evasion is a serious problem for the Brazilian government, resulting in losses amounting to US$280 billion in 2015, making it the second highest in the world. The Receita Federal, Brazil's National Tax Collection Agency, appointed NEC to support its efforts in stemming tax losses.

NEC installed its NeoFace® Watch solution in 14 international airports in Brazil including the Governador André Franco Montoro International Airport (Guarulhos Airport) in Sao Paolo, and Antônio Carlos Jobim International Airport (Galeão Airport) in Rio de Janeiro. The solution is designed to identify potential suspects, who have been registered as being involved in suspicious activity by the agency, at the customs checkpoint.

Countries with Largest Tax Evasion Amount



Source: Richard Murphy, Tax Justice Network

The 14 international airports in Brazil installed with NEC's NeoFace® Watch solution are:

Tancredo Neves (Belo Horizonte, Minas Gerais)
Juscelino Kubitschek (Brasília, Distrito Federal)
Viracopos (Campinas, Sao Paolo)
Afonso Pena (Curitiba, Parana)
Hercílio Luz (Florianópolis, Santa Catarina)
Pinto Martins (Fortaleza, Ceará)
Eduardo Gomes (Manaus, Amazonas)
Augusto Severo (Natal, Rio Grande do Norte)
Salgado Filho (Porto Alegre, Rio Grande do Sul)
Gilberto Freyre/Guararapes (Recife, Pernambuco)
Antônio Carlos Jobim/Galeão (Rio de Janeiro, Rio de Janeiro)
Dep. Luís Eduardo Magalhães (Salvador, Bahia)
Governador André Franco Montoro/Cumbica (Guarulhos, Sao Paolo)
Cataratas (Foz do Iguacu, Parana)

Case Study: Tackling Cybercrimes

CASE STUDY 3

SECURITY OPERATION CENTERS

Hackers are always on the lookout for new ways to bypass control systems of enterprises. Adequate preparedness for cyber-attacks is not easy to achieve as there are unforeseen threats. Organizations can no longer take the passive approach and react only when an attack takes place. Instead, a defensive and proactive approach is needed to monitor, analyze, and plan scenarios, and identify steps to respond to an attack.

To strengthen customer readiness and defense against cyber threats, NEC has established Security Operation Centers (SOCs) in Japan, the Americas, and Europe. As a subsidiary of the NEC Group, the SOCs utilize different time zones across the three regions to provide round-the-clock managed security services that receive and monitor emergency responses to cyber threats from customers around the world. With an interconnected network that shares cyber intelligence on cyber threats, it continuously innovates to manage emerging threats.

Case Studies: Airports and Stadiums

CASE STUDY 4

BIOMETRIC BORDER SCREENING FOR PUBLIC SAFETY

John F. Kennedy International Airport, US

With 30 million passengers in 2015, the JFK International Airport in New York City is the largest international airport in the US with the longest average waiting time.

The sheer volume of passengers passing through the airport creates a challenging environment for airport officials to ensure effective and efficient border safety without compromising passenger convenience and comfort.

To enable customs officers to screen passengers speedily and accurately, NEC installed its facial recognition solution, NeoFace Match, at the airport in 2016. NeoFace Match makes it difficult for passengers to counterfeit a passport and protects legitimate ones from fraud and identity theft. Using one-to-one facial comparison, it matches the photograph taken during customs inspection against the photo stored in a passenger's e-passport chip. The results are shown in a numerical rating system that indicates whether a passenger is legitimate or requires additional screening.

CASE STUDY 5

BIOMETRICS FOR ACCESS CONTROL IN SPORTS STADIUM

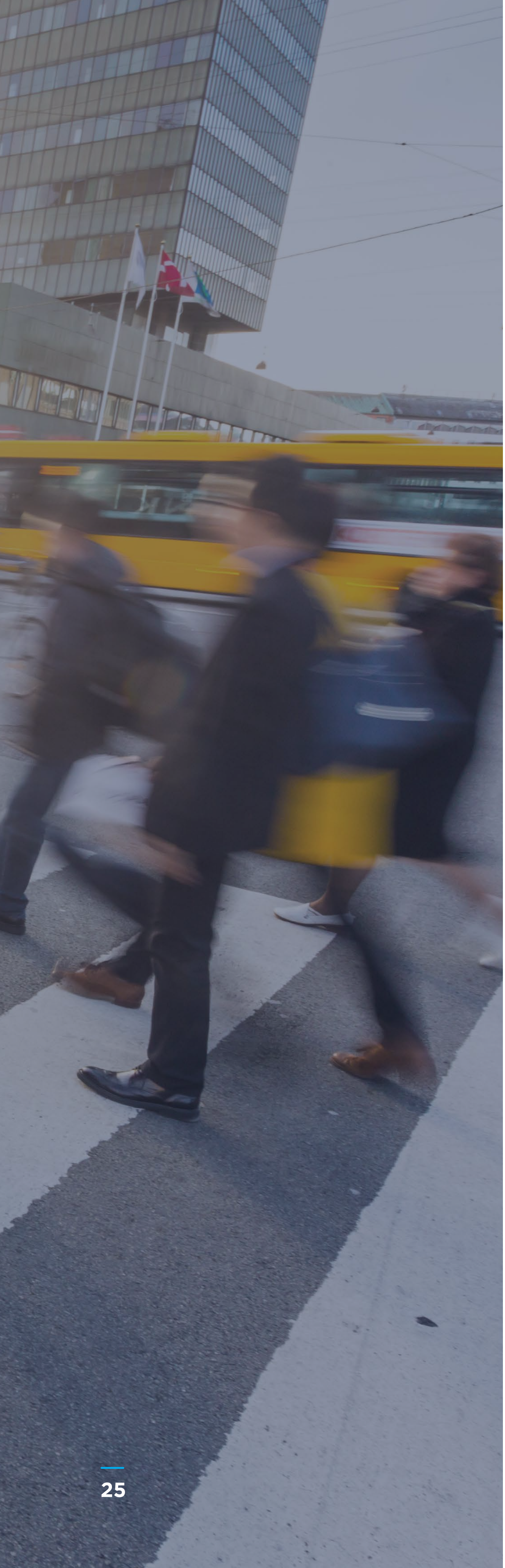
Medellin, Colombia

With a seating capacity of over 40,000 spectators, the Estadio Atanasio Girardot is the third largest stadium in Colombia. The key public safety concern among law enforcement agencies has been around crime, violent behaviour and vandalism during major sporting events.

In 2016, NEC successfully deployed its facial recognition solution that used 170 surveillance cameras strategically positioned throughout the vicinity. It allows security personnel to monitor the situation and observe large crowds from various control centres. Besides detecting disruptive behaviour, NEC's facial recognition solution is able to detect and identify soccer fans who had caused trouble in previous events

05

Key Challenges in Implementation



More and more cities are becoming smarter with the deployment of innovative technologies.

The integration of physical and digital worlds is helping cities to cope with the effects of urbanization and population growth. While digitization of the environmental and business landscapes brings enormous benefits, it exposes agencies, corporations, and citizens to unprecedented risks. To ensure that cities are resilient against security threats, adequate measures are critical to minimizing the risk of a setback in terms of financial losses, physical harm, and loss of confidence in decision-makers. As air gaps in control systems are gradually removed, intruders are finding ways to take control of critical infrastructure that people are heavily reliant upon. The rise in cyber-attacks carried out in the past year alone sends an ominous signal to all decision-makers. As the threat of cyber-attacks looms over critical assets, it is imperative for urban planners to overcome the following challenges:

Existence of legacy systems	High reliance on existing control systems sourced from different vendors and running on proprietary systems that operate in silos breaks down communication among the different systems. Their lack of compatibility with smart technologies create challenges in deploying innovative solutions.
Absence of citizen-driven approach	Technological innovations focus excessively on operating efficiencies and cost savings, which aim to solve problems faced by urban planners. Lack of transparency in their implementation can result in privacy concerns among the community.
Low willingness to collaborate among policy makers	Strong silo mentality coupled with mistrust among policy makers and government agencies cause stakeholders to compete on safe city initiatives independently rather than collaborate toward a common goal.
Preference for status quo	Conservative and risk-adverse urban planners who lack vision choose the conservative, wait-and-see approach to save costs until they encounter a cyber-attack.
Poor clarity in project requirements	Overly ambitious goals covering numerous aspects but lacking in clarity on definitions of stakeholders and project funders, expected outcomes, and challenges in managing expectations cause unnecessary delays.
Lack of human resource with necessary skill sets	Organizations may not have human resource with the necessary skill sets to harness the value of big data analytics and develop meaningful insights to introduce innovative changes and solutions.
Outdated policies	Slow amendments to outdated regulations and practices create barriers in adopting technological innovations, causing enterprises and manpower talent to move to cities that have progressed beyond this hurdle.
Insufficient experience in country-wide deployments	Several safe city projects have been carried out on small scales, hence limiting the experience of urban planners in deploying country-wide implementation for adequate planning, strategizing, and avoiding costly pitfalls.

Source: Frost & Sullivan

With multiple parties striving to make cities safer places to live, it is easy for urban planners to lose focus after a while. Many of them commence with realistic plans to start small and scale up. However, as more stakeholders come on board, requirements and considerations are inclined to increase, with unexpected challenges likely to occur. Urban planners with insufficient experience in the implementation of safe city initiatives may not be able to anticipate the potential challenges that can have costly consequences.

06

Recommendations in Deploying Safe City Solutions

A UTOPIAN VISION OF A SAFER CITY DRIVEN BY COMMUNITY AND STAKEHOLDERS

Focusing solely on deploying the best technological solutions does not necessarily make a city more secure. People are increasingly aware of authorities continuously monitoring and tracking their movements. Stakeholders require urban planners and decision-makers to be more transparent about the data on individuals they are capturing and how the data is used.

As people become more critical of the authorities, getting the active support of all stakeholders is even more essential. A mindset shift from a top-down decision-making approach to one that facilitates the roles of stakeholders on the ground is required. A bold vision of the future entails evolving from an efficiency-driven city to one that embodies the following characteristics.

An Inclusive Society where authorities no longer dictate the safe city landscape. Instead, they relinquish some command-and-control to take on the role of facilitator that brings together various stakeholders in a constructive dialog. Partnerships among private enterprises, entrepreneurs, non-profit entities, and community activists are likely to drive innovative solutions and policy modifications along every stage of the safe city program.

Law enforcement officials can become more effective with the support of the community. Citizens could work collectively with the authorities in reducing crime and social unrest. Commercial entities, households, and individuals can also share video footage of incidents captured on their devices and surveillance cameras to supplement authorities with robust intelligence resources. People should have a strong say in revising policies on data privacy and protection and no longer feel threatened about surrendering their data to the authorities.

An Empowered City that enables people across a broad spectrum of sectors to offload repetitive tasks to automation to focus on building new skill sets. Tertiary institutions should work closely with the industries to identify and equip people with skills to cope with technological disruptions. Rather than being displaced by robots, professionals undergo reskilling to make better use of cutting-edge technologies to produce better outcomes not possible before.

A Safe City is better equipped to absorb and rebound from the impact of external forces. Policymakers no longer work in silos, but collaborate actively by sharing data and tackling common problems via an integrated platform. Integrating multiple forms of threats raises the effectiveness of law enforcement, public safety, crime prevention, and disaster management. Agencies are able to carry out scenario planning and anticipate incidents together. They adopt a consistent approach, so all parties know what to expect and what to do in the event of a crisis or attack. People are calm in the face of an unexpected event if they have been involved in the planning and deployment of the contingency measures.

07

The Last Word

Accelerating urban development is necessitating an urgent response to addressing multiple forms of threats proactively and identifying a technology vendor with a proven track record in leading safe city solutions. Screening vendors involves a broad understanding of their best practices, resources, and expertise. You want somebody reliable that brings strong technical capabilities, established strategic partnerships, and thought-leadership to anticipate when, where, and the extent of the next security attack.

NEC displays extensive capabilities in advanced technologies and solutions that are aligned with the challenges facing organizations. Its leadership in biometrics, video analytics, and big data analytics are incorporated into diverse verticals-focused solutions addressing security challenges under different scenarios. With years of experience in security solutions, NEC remains committed to its “Safer City” vision with solutions that bring about a win-win outcome for all stakeholders.

Some photos are for illustration purposes only.

FROST & SULLIVAN

NEXT STEPS

Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

Visit our **Digital Transformation** web page.

Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY

3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

SAN ANTONIO

7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON

Floor 3 - Building 5,
Chiswick Business Park,
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

SINGAPORE

100 Beach Road
#29-01/11, Shaw Tower
Singapore 189 702
Tel +65.0.6890.0999
Fax +65.0.6890.0988

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041