Cyber Security
A necessary pillar of Smart Cities
2016

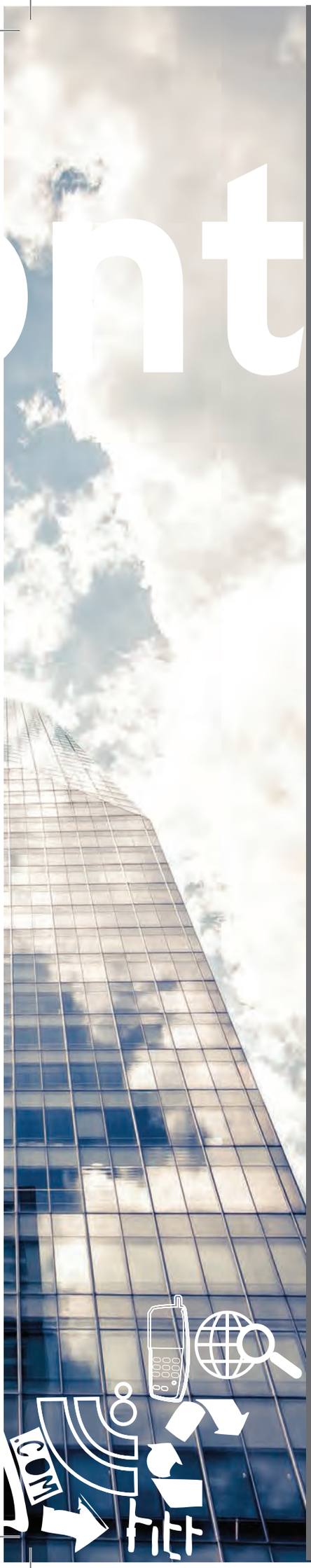
INDIA SECURITY CONFERENCE

ASSOCHAM INDIA

EY
Building a better working world

Co

ntents



Message

MP International is very honoured to partner EY in India for our inaugural India Security Conference 2016. Held alongside InfoComm India, the nation's foremost pro-AV and ICT exhibition and conference, the 2-day India Security Conference aims to address challenges and solutions for "Building Safe and Secure Environments with Intelligence, Analytics and Mobility".

MP International is very excited to be providing a knowledge exchange platform in the Security space. Besides India Security Conference, MP International organizes two other security events in our portfolio - Myanmar Security Expo, which reaches out to buyers of security products and services in the Indochina markets; and INTERPOL World, an event owned by INTERPOL and managed by MP International.

Safe Cities and Cybersecurity are hot button issues, in both the public and private sector. As highlighted in EY's 14th annual Global Information Security Survey, it confirmed that information security is one of the most important issues facing organizations today. In another recent study[1] it was reported that the average consolidated total cost of a data breach grew from USD3.8 million to USD4 million. The report also indicated that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from USD154 to USD158.

The rate of urbanization has moved cities to adopt and implement "Smart City" programmes. Innovative solutions and technologies are much sought after to ensure that security risks risks in cities are minimised. The limited or lack of understanding of such innovations will lead to improper implementation and execution of the ensuring that a smart city is safe.

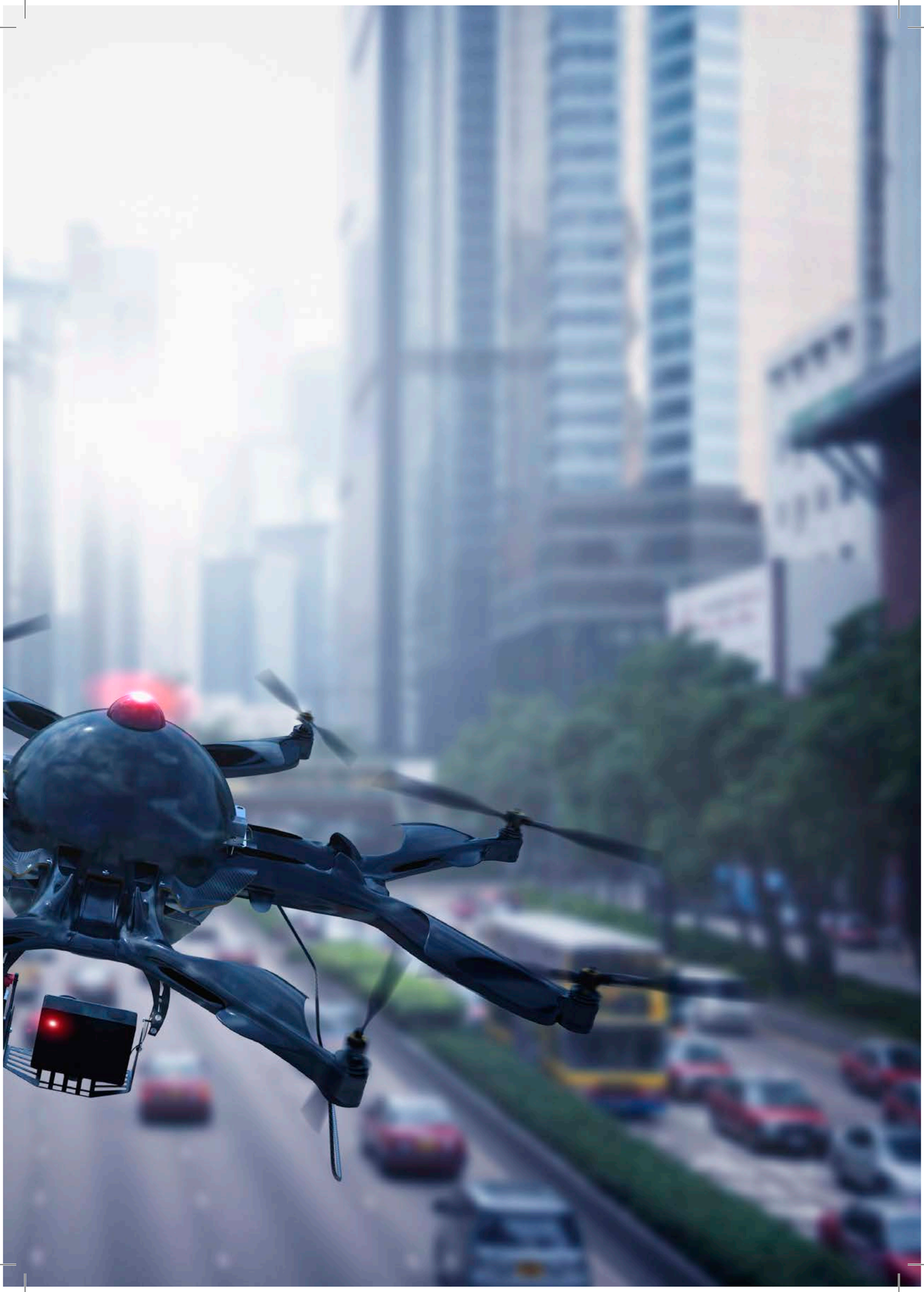
So, how can both public and private sectors combat these threats and challenges? What are some of the pitfalls within our organisations we have to look out for? What are some of the latest solutions? Are there examples that we can learn from? These, and more, will be addressed at our 2-day India Security Conference 2016.

We thank EY India and our Conference Partner, ASSOCHAM for jointly sharing insights for the publication of this report.

We hope everyone has a fruitful discussion at India Security Conference 2016.

Jack Chia
Executive Director
MP International

[1] 2016 Ponemon Cost of Data Breach Study



Fore

Over the past few decades technology has begun to play a very important role in our day to day lives. Our internet enabled gadgets have changed the way we work, play or even carry out daily chores. Digitalization impacts almost everything from personal lives, education, health, business and trade, physical infrastructure, governance to national security.

Information and communications technology has become indispensable to the modern life, we critically depend on information and communication infrastructure in governing our personal lives, our societies, conducting business and running critical infrastructure. Hence more governments are taking an interest in adopting "smart" concepts, for management of energy, water, transportation, waste, surveillance and security etc.

Smart cities move from being a buzzword to reality as the market has evolved into its next stage. As more governments begin to adopt "smart" concepts, most find it challenging to keep pace with rapid changes in the digital world and the continued evolution of their service delivery models.

The increased complexity of city's systems, interdependencies, globally connected social, economic and political sub systems has increased the vulnerability of a city's security. The cyber threats get magnified as infinite supply of data becomes more integral to a wide array of operations.

The interface between urban growth, technology, infrastructure and capital requirement presents a unique set of opportunities and challenges to the implementation of Smart cities. The challenges cities face generates demand for investment in the physical, economic, institutional and social infrastructure. The report tries to highlight the various parameters of a smart city, existing security challenges and possible solutions.

Burgess Cooper
Partner, Ernst & Young LLP

word

Today Cyberspace touches almost every part of our daily life. Be it through broadband networks, wireless signals, local networks or the massive grids that power our nation.

The threat from cyber attacks and malware is not only apparent but also very worrisome. There cannot be a single solution to counter such threats. A good combination of Law, People, Process and Technology must be established and then an effort be made to harmonize the laws of various countries keeping in mind common security standards.

ASSOCHAM lauds the efforts made by the Government of India under the leadership of Shri Narendra Modi, Hon'ble Prime Minister of India to ensure a secure and resilient cyber space for citizens, businesses, and the Government.

We at ASSOCHAM, have been discussing and deliberating with the concerned authorities and stakeholders about the need for security compliance and a legal system for effective dealing with internal and external cyber security threats.

ASSOCHAM is privileged to be the Member of the Joint Working Group (JWG) on Cyber Security set up by National Security Council Secretariat (NSCS), Government of India, Member of Cyber Regulation Advisory Committee and Member of Joint Working Group on the Digital India both set up by Ministry of Communications and IT, Government of India.

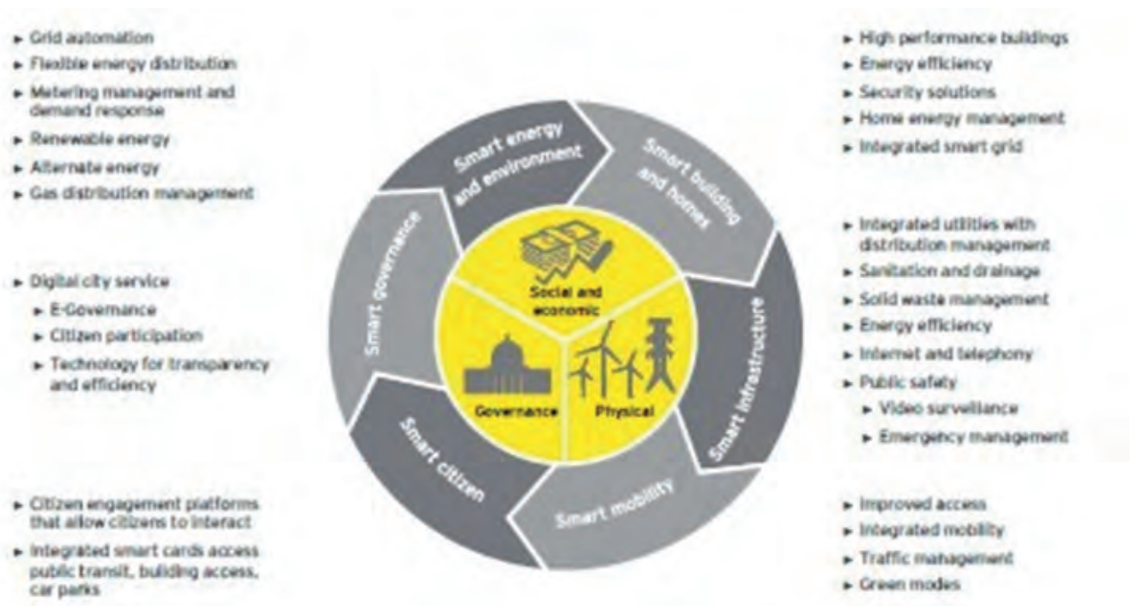
We convey our very best for the success of the INDIA SECURITY CONFERENCE 2016 "CYBER SECURITY & SAFE CITIES" being organized in association with ASSOCHAM and hope the Conference provides more insight to emerging cyber related challenges and their appropriate solutions for further securing the cyber space.

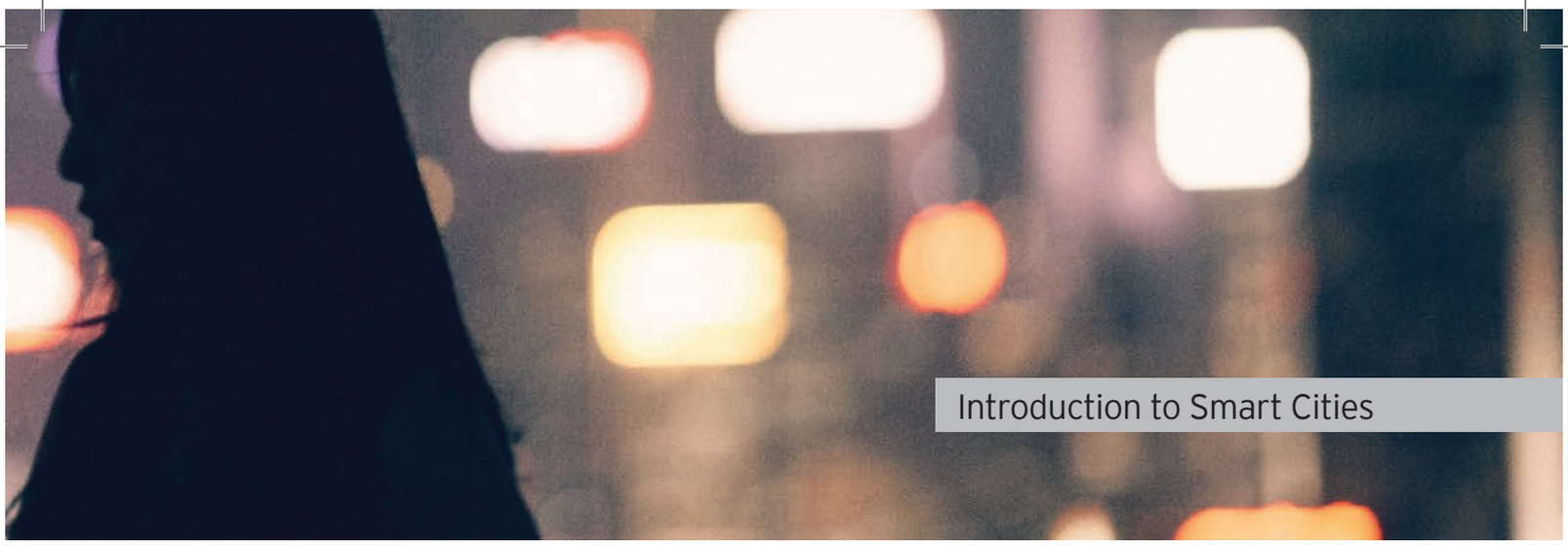
D.S. Rawat
Secretary General
ASSOCHAM

Introduction to Smart Cities

The Smart Cities Mission is a bold new initiative by the Government of India to drive economic growth and improve the quality of life of people by enabling local development and harnessing technology as a means to create smart outcomes for citizens.

A smart city is an urbanized area where multiple sectors cooperate to achieve sustainable outcomes through analysis of contextual real-time information shared among sector-specific information and operational technology systems.





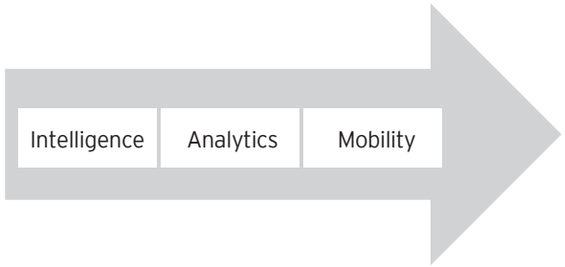
Key Parameters of a Smart City

- Smart Energy: Digital Management of Energy; Smart grids, Smart meters, Intelligent energy storage
- Smart Buildings: Automated Intelligent Buildings; Advanced Heating Ventilation and Air conditioning systems (HVAC), Lighting Equipment
- Smart mobility: Intelligent mobility; Advanced traffic management system (ATMS), Parking management, ITS-enabled transportation pricing system
- Smart Technology: Seamless Connectivity; 4G connectivity, Super broadband, Free Wi-Fi
- Smart Infrastructure: Digital Management of Infrastructure; Sensor networks, Digital water and waste management
- Smart Governance and Smart Education: Government-on-the-Go; e-Government, e-Education, Disaster management solutions
- Smart Healthcare: Intelligent Healthcare; Technology, Use of e-Health and m-Health systems Intelligent and connected medical devices
- Smart Citizen: Civic Digital Natives; Use of green mobility options, Smart lifestyle choices
- Smart Security: Intelligent Threat Detection; Surveillance, Biometrics, Simulation modelling and crime protection, Advanced proactive antivirus protection

The global smart city market is expected to reach US$1.565 trillion in 2020, with one-half of smart cities from North America and Europe*. E-Services to citizens, such as e-Payments, e-Exchange, e-Sharing, etc., will empower citizens with real-time access to personal data and related services.

(*Source: Frost and Sullivan)

Fundamental to the creation of smart cities is the generating, analysing and sharing of large quantities of data. Indeed the main aim of smart cities technologies is to make cities data-driven; allowing city systems and services to be responsive and act upon data in real-time.



Intelligence: the first and most important stage of security is surveillance and intelligence gathering. This calls for equipment such as CCTVs and Biometrics hardware and software to collect the essentials in its raw, unprocessed form. Secured network for transmission of data is important to ensure non-tempering of data.

Analysing Data collected: Analytics help digest, decode and make sense of the terabytes of information and data collected, by providing secured storage, analysis and forensic tools. Change from byte-sized to bite-sized for effective prevention against threats or reaction to a calamity and provide situational awareness.

Mobilising the Resources: There is human intervention in any security installation with physical security apparatus from perimeter protection to communication devices for personnel on the move. The effective mobilisation of people and equipment is crucial to the entire infrastructure of a steadfast and secured location.

Introduction to Smart Cities

The interconnectivity of people, devices and organizations in today's digital world, opens up new vulnerabilities – access points where the cyber criminals can get in.

The multiplying effect of today's cybersecurity challenges presents an opaque universe of threats that often come from unexpected or unforeseen domains which have an escalating effect.

- The speed of change – can the Smart City's cybersecurity keep pace?
- New product launches, mergers, acquisitions, market expansion, new technology
- A network of networks has made data accessible everywhere, any time
- One vulnerable device can lead to other vulnerable devices
- Traditionally closed operating systems can be accessed externally
- Cloud vulnerabilities and Big data – storage and server security issues
- Bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications.

Pillars of a Smart City

1. Institutional Infrastructure refers to activities relating to governance, planning and management of a city. ICT has provided a new facet to this system making it citizen centric, efficient, accountable and transparent.
2. Physical Infrastructure refers to its stock of cost-efficient and intelligent physical infrastructure such as the urban mobility system, high speed broadband infrastructure, the housing stock, the energy system, the water supply system, sewerage system, sanitation facilities, solid waste management system, drainage system, etc. which are integrated through use of technology.
3. Social Infrastructure relates to components that enable development of human and social capital, such as the education, healthcare, entertainment, etc. It also includes performance and creative arts, sports, the open spaces, children's parks and gardens.
4. Economic Infrastructure pertains to developing proper infrastructure that generates employment opportunities and attract investments.

The evolution of smart cities and the increasing need for connectivity and communications will mean that more information is being gathered and interpreted. This analysis then provides intelligence on how to act and react to critical situations. The transmission, analysis and storage of big data will trigger the need for information security at all stages.

Safety of Smart Cities

Smart Cities have smart (intelligent) physical, social, institutional and economic infrastructure while ensuring centrality of citizens in a sustainable environment. It is expected that such a Smart City will generate options for all residents to pursue their livelihoods and interests meaningfully and with joy. (According to the Draft Government Concept note on Smart City Scheme)

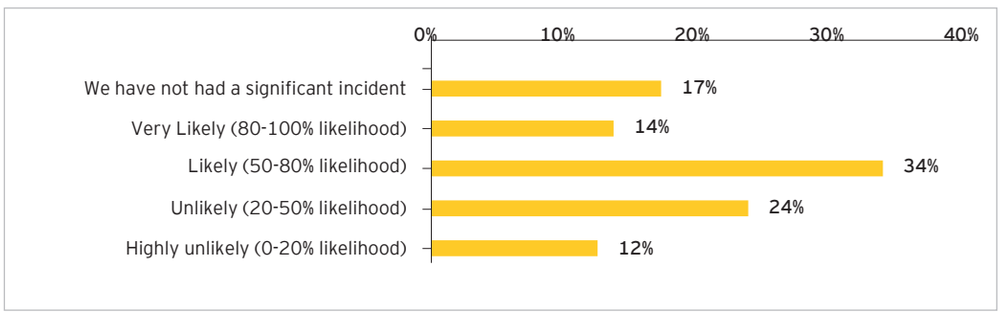
Smart surveillance technology or analytics to manage the crowd, traffic, cyber security, data privacy, building code to manage natural/man-made disasters etc, are factors that would make a city safe and secured for a citizen to live in.

The rise of cyber threat

Effective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding due to the need for collaboration with external partners and businesses, the existing security defences are coming under increasing pressure.

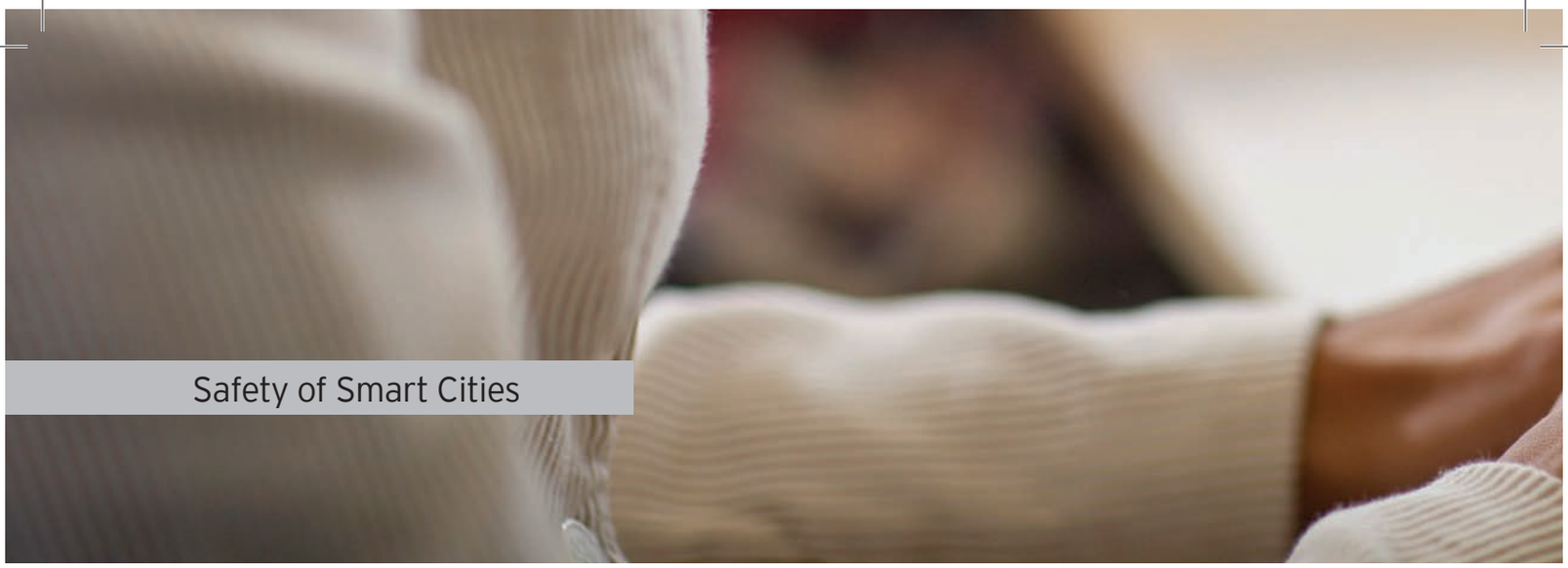
Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information – they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property.

Every day, their attacks become more sophisticated and harder to defeat. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years' time, or in 10 years' time; we can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of this threat fade, new sources will emerge to take their place. Despite this uncertainty – in fact, because of it – we need to be clear about the type of security controls needed



**Statistics from EY LLP GISS Survey 2015*

In response to EY LLP GISS survey 2015, 56% of respondents say that it is "unlikely or highly unlikely" that their organization would be able to detect a sophisticated attack.



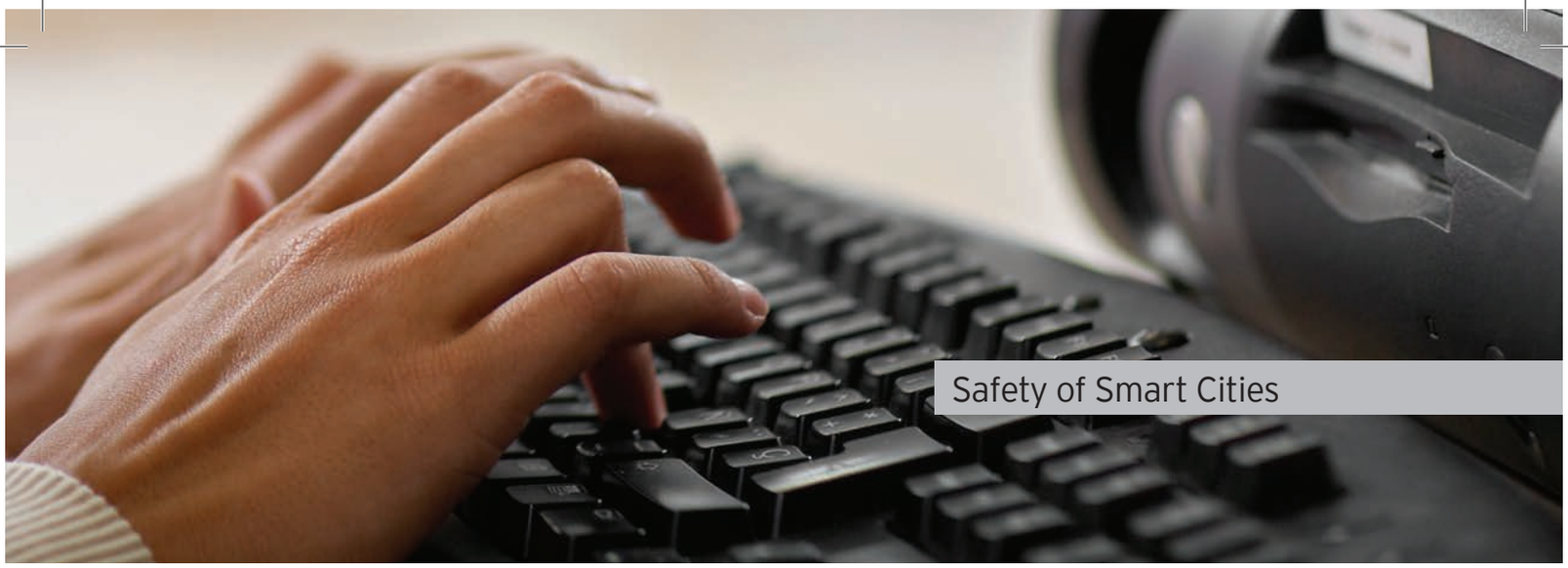
Cyber-attacks have transformed the risk landscape

It's important to remember that cybersecurity is a city-wide issue and not just a technology risk. Since many opportunities for IoT will arise through technological integration and collaboration, which will continue to increase in complexity – this complexity breeds risk.

A standard approach to risk management assumes that the trust boundary is already defined. What is missing in the risk-focused and techno-centric approach is everything related to the management of trust, i.e., the new functions and processes, and the new policies and structures required to expand the risk boundary.

Risk Landscape

To effectively manage the risks in a Smart City, it is important to clearly define the limits of that ecosystem. We also needs to decide what we are willing to manage within those limits: is it just the risks faced by groups of people that are in the city itself, or should we also try to influence the mitigation of risks faced by people/data outside the limits defined.



Security Challenges in Smart Cities

Data Privacy and protection concerns: Privacy is considered as a basic human right and is protected by national laws in different ways. Privacy concerns include the acceptable practices with regards to accessing and disclosing personal and sensitive information about a person. Sensitive information can relate to a number of personal facets such as any information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Smart city technologies capture data relating to all forms of privacy and drastically expand the volume, range and granularity of the data being generated about people and places. Privacy can be threatened and breached by a number of practices which are normally treated as unacceptable, however are part of operations in a smart city eco system.

- Surveillance: Watching, tracking, listening to or recording a person's activities
- Aggregation: Combination of various aspects of data about a person to identify a trend or pattern of activities.
- Data leakage: lack of data protection policies can lead to leakage or improper access of sensitive information
- Extended usage: use of data collected for period longer than stated or for purposes other than the stated purpose without the subject's consent

Insecure Hardware: One of the major concerns about smart cities sensors in the equipment; buildings etc. are insecure and not tested thoroughly. Owing to lack of standardization of IoT devices, the sensors are prone to hacking. Notorious individuals can hack the sensors and feed fake data, causing signal failures, system shutdowns etc.

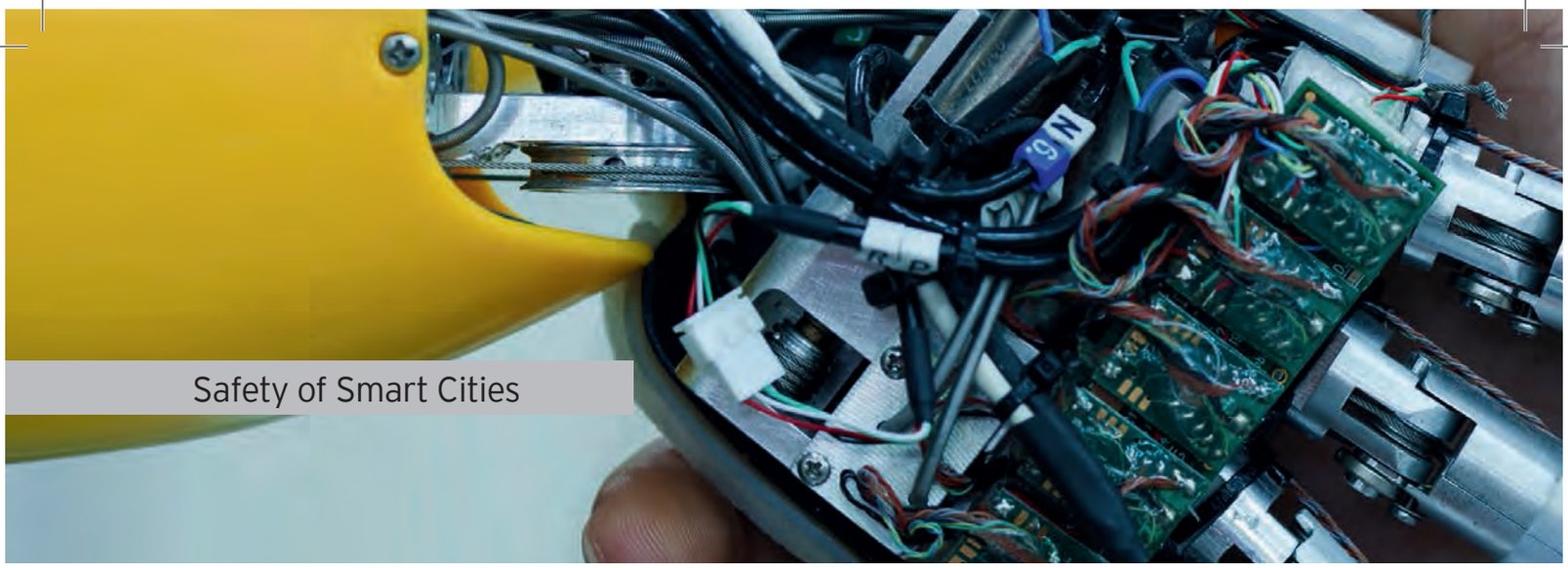
Larger Attack surface: Smart city operations utilize complex, networked assembly of ICT infrastructure to manage various services. Any device that is connected to the network is vulnerable to being hacked; the number of potential entry points is multiplied in Smart Cities. By compromising a single device, it is possible to attack the entire system or network. The vulnerability of systems is worsened by a number of issues including weak security and encryption; the use of insecure legacy systems and poor maintenance; cascade effects; and human error.

Bandwidth consumption: Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there are possibilities of security lapses. The bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications, which also operate on the megahertz frequencies like radio, television, emergency services, etc.

Application risk: Apps have accelerated the integration of mobile devices within our daily lives. From mapping apps, to social networking, to productivity tools, to games, apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today. While apps demonstrate utility that is seemingly bound only by developer imagination, it also increases the risk of supporting Bring Your Own device (BYOD) in a corporate environment.

As the organization enables employees to bring their own devices, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

- Malicious apps (malware): the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes
- App vulnerabilities: apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses



Safety of Smart Cities

Simple Bugs with Huge Impact: a simple software bug can have huge impact. As Smart Cities will run on hundreds of systems and devices managing critical services, a simple software bug can have huge impact. For instance November 2013 Bay Area Rapid Transit (BART): major software glitch, service was shut down by a technical problem involving track switching, it affected 19 trains with about 500 to 1,000 passengers on board.

Getting ahead of cyber crime

Early warning and detection of breaches are decisive to being in a state of readiness, meaning that the emphasis of cybersecurity has changed to threat intelligence. A state of readiness to deal with cyber-attacks requires behaviours that are thoughtful, considered and collaborative. No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience and limit damage from any given attack.

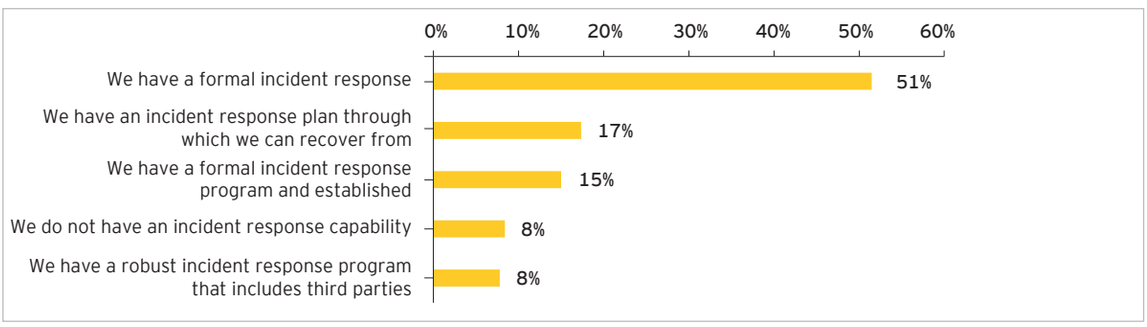
A state of readiness includes:

- Designing and implementing a cyber-threat intelligence strategy to support strategic decisions and leverage the value of security
- Defining and encompassing the organizations extended cybersecurity ecosystem, including partners, suppliers, services and business networks
- Taking a cyber-economic approach – understanding your vital assets and their value, and investing specifically in their protection
- Using forensic data analytics and cyber threat intelligence to analyse and anticipate where the likely threats are coming from and when, increasing readiness
- Ensuring that all the stakeholders understand the need for strong governance, user controls and accountability

Governments may not be able to control when information security incidents occur, but they can control how they respond to them – expanding detection capabilities is a good place to start. A well-functioning security operations centre (SOC) can form the heart of effective detection.

Managing cyber threats according to strategic priorities must be the focus of the SOC. By correlating relevant information against a secure baseline, the SOC can produce relevant reporting, enabling better decision-making, risk management and business continuity.

An SOC can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.



As per results of EY LLP GISS 2015 survey, 37% respondents say that real time insight on cyber risk is not available. Also only 8% organizations claim to have a robust incident response program that includes third parties and law enforcement and is integrated with their broader threat and vulnerability management function.

Components of a Safe Smart City

Surveillance system and equipment:

The aim of smart city is to provide shared security presence and real time surveillance with the use of video cameras. The cameras collect data in image or video format which may be monitored from a central location, and allow first responders to act instantly in an emergency situation.

Video analytics

Video analytics is the capability of automatically analysing videos to detect certain objects, behaviour, spatial and temporal events. This is used in a wide range of domains, including entertainment, Health care, surveillance, home automation etc. These Video analytics tools can be used with a wide range of modules for various purposes and can work as a proactive monitoring tool, triggering alarms to signal immediate attention of concerned teams.

Data centre

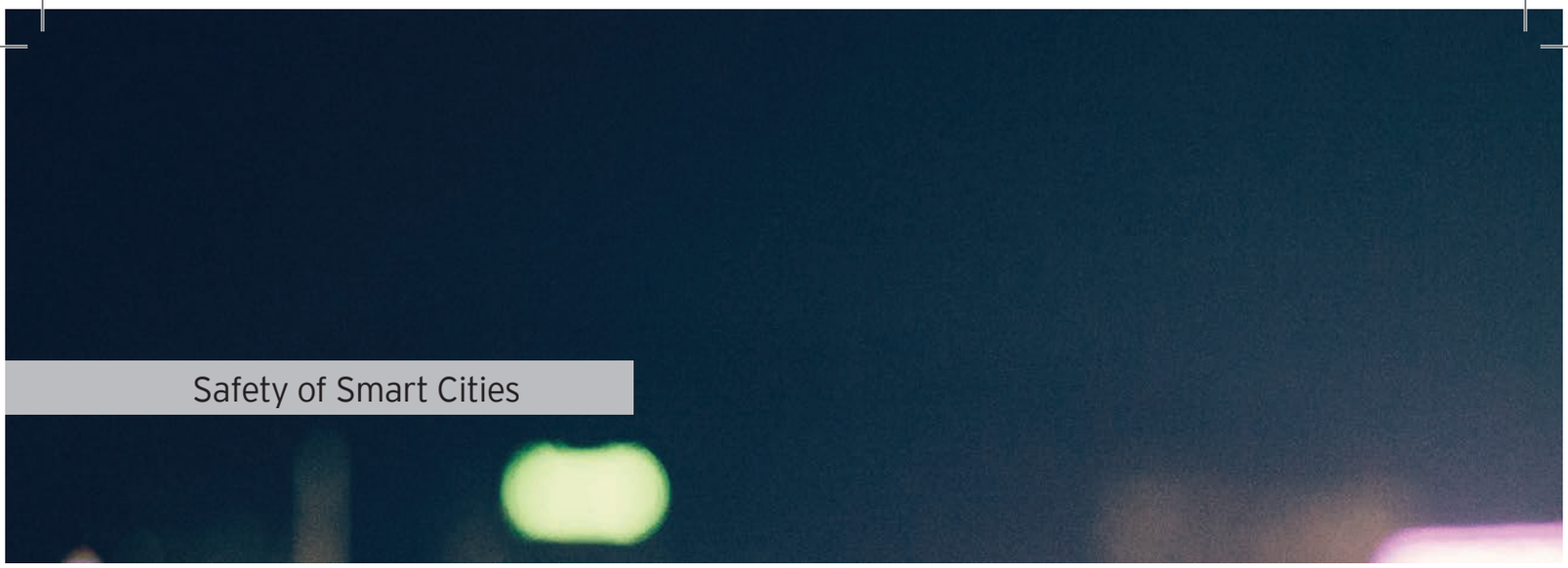
The data centre is the centralised storage space for all the data collected from the multiple sensors in the network. The data centre provides real time data to monitoring centres for effective operations. The data centre hosts applications for the operation of video management, analytics and traffic control etc. The design of data centre depends on the kind of applications that are run in the smart city.

Command Centre

The command centre provides an infrastructure that can assess the integrated information provided by the data centre such as live video for incident response. It aids in quicker analysis of data for better decision making.

Knowledge Transfer

It is important to disseminate the required knowledge and skills for the smooth operation and implementation of the smart city initiatives. The concerned staff needs to be trained in operating the new and redesigned services and efficiently deliver the outputs.



Possible Solutions to challenges

Technology Solutions:

As mentioned previously, smart city technologies have large attack surfaces that have a number of vulnerabilities, especially in systems that contain legacy components using old software which has not been regularly patched. Technology solutions aim to use best practices to mitigate these risks

This includes:

- End-to-end encryption
- Strong password policy
- Up-to date firewalls, anti-virus
- Audit logs
- Isolation of trusted resources from public resources (DMZ)
- Implement manual over rides on all systems

The aim is to reduce the attack surface as much as possible and to make the surface that is visible as robust and resilient as possible.

Move from security as a cost, to security as a plus

Security is usually positioned as an obligatory cost – a cost to pay to be compliant, or a cost to pay to reduce risk. But moving to a model of security as risk and trust management implies looking upon security as an enabler; for example, managing public data access leverages the monetary value of the data instead of focusing on the protection of the data itself. In fact, this transformation means enabling the development of even more extended networks of networks, of more and new forms of collaboration and mobility, and of new business models. "Security as a plus" should be a mainstay of the business.

Continually learn and evolve

Nothing is static – not the criminals, not the eco system or any part of its operating environment – therefore the cycle of continual improvement remains. Become a learning organization: study data (including forensics), maintain and explore new collaborative relationships, refresh the strategy regularly and evolve cybersecurity capabilities.

Disaster recovery and back-up services

Data centres, either on site or off site, are at the heart of smart cities. Disaster recovery is a critical part of the data centre's architecture. If servers go down, is it important that systems are brought back online as soon as possible and, once those systems are back up and running, need to have all their previous workloads operational. It is important to identify the right level of back-up required for various services.

Data back-ups should be done regularly, and according to the best practices, should be done off site. This helps in data protection in case of physical security breach at the data centre.

International Leading Practices

- **Data Protection Directives**: Recently the European Parliament adopted The EU General Data Protection Regulation (GDPR) which aims to strengthen and unify data protection within the European Union. When GDPR comes into effect in May 2018, the EU residents will gain more control of their personal data, all organizations will have the same rules and will report to one supervising authority. There are stringent restrictions on profiling, and definition of "consent" to collect/process data.
- **Digital access control systems**: DACs have to be built to ensure only the authorized officials have access to smart city data and the networks. DACs are crucial to protect the city's services from cyber threats, hacking or alterations to data.

  In these DACS, different levels of entry can be allocated to different parties in order to ensure that the right people see exactly the required amount of information. Segregation of duties and updated database of who has access to the data and networks will help identify causes when a breach does happen.
- **Privacy Enhancing Technologies**: PETs provide individuals with tools, applications and mechanisms to protect their personally identifiable information (PII) and dictate how PII should be handled by different services. PETs have been defined by the European Commission as 'a coherent system of information and communication technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data without losing the functionality of the information system.'

  PETs include relatively simple tools such as ad blockers, cookie blockers and removers, malware detection and interception, site blocking, encryption tools, and services to opt-out of databases held by data brokers. In general, these kinds of PETs are aimed at protecting PII on websites and smartphones and managing how data are handled by data brokers.

Governance and management Solutions

A critical component of well-run smart city is its governance and management structure and processes. Governance provides the framework through which strategic direction is deliberated and set, and regulation and oversight administered. On the other hand management consists of leading and driving forward initiatives and stewarding the day-today running of services.

Putting in place strong principle-led governance and management is therefore a prerequisite for creating a smart city that seeks to maximise benefits while minimising harms. However to date, there are very few documented cases of such governance and management structures being constituted. Instead, smart city initiatives have been procured and developed with little coordinated consideration of privacy and security harms and slotted into existing city management in an ad hoc fashion with minimal strategic oversight.

International Leading Practices

Given the potential harms and the associated costs that can arise, this piecemeal approach needs to be discontinued to be replaced with a more strategic, coordinated approach that consists of interventions at three levels: vision and strategy (smart city advisory board); oversight of delivery and compliance (smart city governance, ethics and security oversight committee); and day-to-day delivery (core privacy/security team and computer emergency response team). This approach recognises that there is a need for collaboration between experts in different domains to ensure sharing of knowledge and shared learning.

Smart city advisory boards:

In response to the privacy implications of smart city technologies and a number of criticisms of the city's data practices, Seattle has established a Privacy Advisory Committee (PAC) to assess the ways in which the city authorities generate, store and use data, and to consider issues such as confidentiality, anonymity, archival procedures, deletion, sharing and publishing as open data, and the ability to conduct forensic internal audits. The PAC has published a set of basic privacy principles. In essence, these principles simply confirm that the city is following FIPPs (fair information practice principles) and its already existing legal obligations. They are complemented by a much more detailed privacy statement that sets out the city policy on privacy issues.

Transparent data policy:

A local government body responsible for public transport in Europe and coordinating travel for millions of passengers daily, generates and manages a massive amount of data from a diverse set of sources.

The organization has adopted a transparent approach to data privacy and data protection policies, which are published on their website. For each type of data detail: what personal information they hold, why they collect that information, how they use the information; the length of time they keep it before deleting (varies from 24 hours to 7 years, depending on type and purpose, how they secure it, how they share it, if any of the data are processed overseas, how someone can access the data held about them, any relevant privacy notices.

City Computer Emergency Response Teams (CERTs)

CERTs consist of a team of key personnel, drawn from the core privacy/security team, IT services, smart city initiatives and emergency services, that spring into action when a smart city technology experiences a cybersecurity incident and is hacked and records stolen or the system disrupted or terminated.* CERT is similar to other emergency response teams that tackle other city events. CERTs prepare detailed plans of action and accountability/responsibility in the case of different types of incidents.

** Source: Cerrudo, C. (2015) An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks.*

Private Public Relationships for Smart City Management

Public- Private Partnerships According to the World Bank are typically medium to long term arrangements between the public and private sectors whereby some of the service obligations of the public sector are provided by the private sector, with clear agreement on shared objectives for the delivery of public infrastructure and/ or public services.

Smart PPP contracts including the use of smart technologies may be established in Smart City projects such as the installation of a network of sensors or the development of Open Data policies, Data leakage protection, analysing and mitigating cyber threats etc.

In developing Smart Cities, the local government may partner both with big service and technology providers, as well as with small and medium-sized local firms or start-ups. Smart PPPs may involve comprehensive reforms of the legislation and procurement procedures. There is a wide range of legal arrangements available for the different parties to enter into a partnership for better implementation of secure Smart Cities.

Conclusion

Smart Cities present a huge market opportunity of $1.56 trillion, with more than 26 smart cities expected to be established by 2025. Smart Cities aim to provide wide range of benefits such as better transportation, waste management, energy management, which will considerably improve the living standards for the citizens. The challenge is to acknowledge that there are a set of issues and concerns that need to be addressed, and to find and adopt solutions to these that also enable the benefits of smart city technologies to be gained.

Smart city models should boost development while not compromising on data privacy and security. Smart city deployments involve multi-faceted developments, carried out by a diverse ecosystem of providers involving cutting-edge technology including critical and complex ICT implementations.

However, increasing ICT complexity implies increasing vulnerability, both to malicious attacks and unintentional incidents. By having robust security and information protection framework and policies in place, safety for both citizens and enterprises can be ensured.

It is now important to develop the good practices identified so far, to build on and conceptually enhance the suggested solutions. Once the solutions are deployed in practice, these need to be evaluated in turn and iterative learning process needs to be applied.

To aid in implementation and governance of the smart city projects, the government can enter into Public Private Partnerships, to employ the expertise of the private sector in order to deliver the benefits of smart cities efficiently


YO!

Notes

Notes

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1609-079
ED None

VS

EY refers to the global organization, and/ or one or more of the independent member firms of Ernst & Young Global Limited