



Cyber Security in Smart Cities

KPMG Point of View

KPMG India

February, 2019



The world today is urbanized...

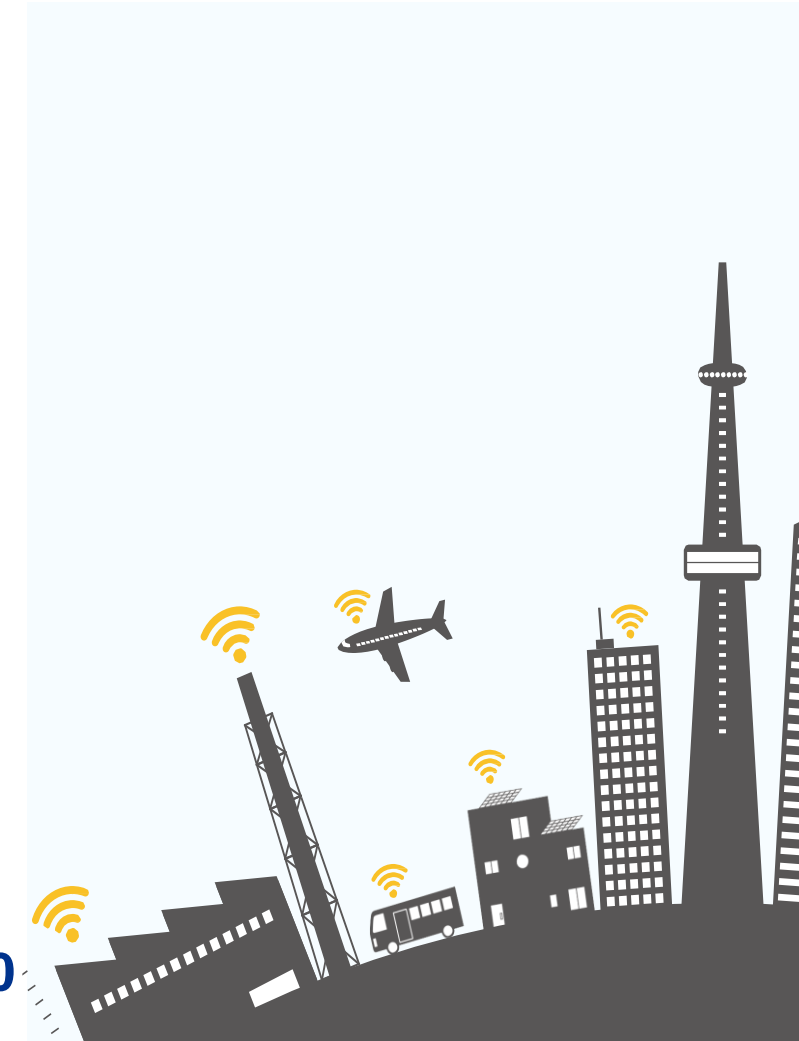
~ 1.3 million people are moving to cities each week

65% of world's population is likely to be city dwelling by 2040

There are 21 mega cities with over 10 million people...
...by year 2025 there will be 30+ mega cities

80% of economic growth will occur in cities...
...consuming 60-80% of world's annual energy needs

India story, cities as engines of growth, nearly 40% of India's
population would be living in urban areas by 2030





//

India is at helm of urban transformation,
with population of 377.1 million
(~31.6%) utilizing urban infrastructure

//

The need for *sustainable* smart cities



Embodiment of Smart Cities

Smart cities represent civil infrastructure augmented with a digital arm converting city assets into services, to improve urban living standards and reduce environmental impact of growing populations...the 4M's



Mobilised

- State of Art Infrastructure with green spaces, roads and buildings
- Utilities like water, electricity, gas, connectivity
- Social spaces and common assets



Monitored

- Centrally monitored services through a command and control centre
- City surveillance for security while maintaining privacy of residents



Managed

- One window services for all city utilities
- Intelligent services with proactive response
- Collaborative service utilization and management



Measured

- Fund management and monetisation of services
- SLAs definition for city services
- Data analysis and cityservices trends

Infrastructure and process
Smart solutions in alignment with city vision

Build and operate
Implement solutions with business process mapping

Optimise
Audit and build capacity for efficient management

For 'Smart' solutions



Egovernance & Citizen Services

- Citizen engagement, public information and grievance management
- Electronic service delivery
- Surveillance, monitoring and crime control

Smart Urban Mobility

- Intelligent and integrated traffic management systems
- Smart parking
- Intelligent and integrated multi-modal transportation systems

Smart Waste Management

- Waste recycling, reduction and re-use through conversion to energy, fuel and compost

Smart Healthcare

- Smart patient health management & healthcare
- Data based public health intercessions, infectious disease surveillance, care search & scheduling
- Remote patient monitoring & telemedicine

Smart water management

- Monitoring water sources and water distribution systems for optimising water resource usage, ensuring water quality and minimising leakages

Smart Trade and Economy Facilitation Centers

- Digital business licensing and permits
- Digital land use, building registration and permits

Smart Energy Management

- Smart metering, smart grids and management of power
- Smart and efficient channelising of renewable energy
- Energy efficient and green buildings

Smart Skill Development Centers

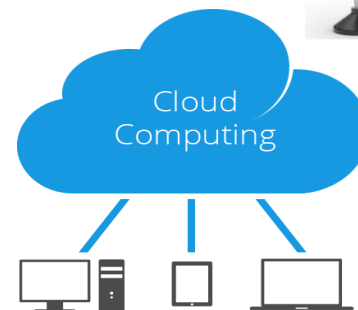
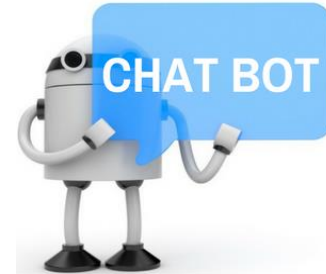
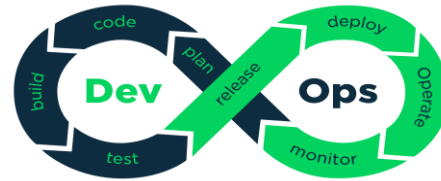
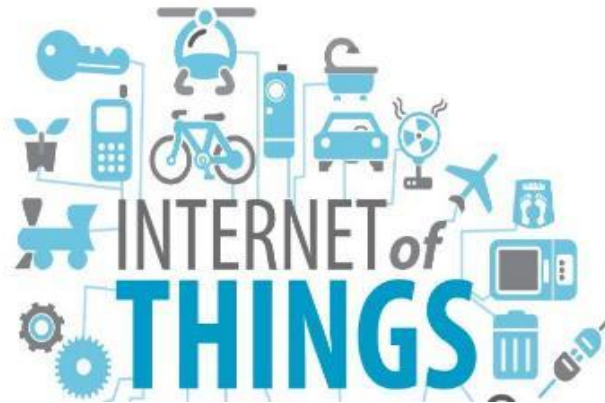
- Personalised education and online training programs
- e-career portals

Anchored on Technology



IoT-based devices provide significant opportunities and it is imperative to have them operate in a secure environment to realise all the benefits

New technology



And the associated cyber risks

Traditional Security Threats

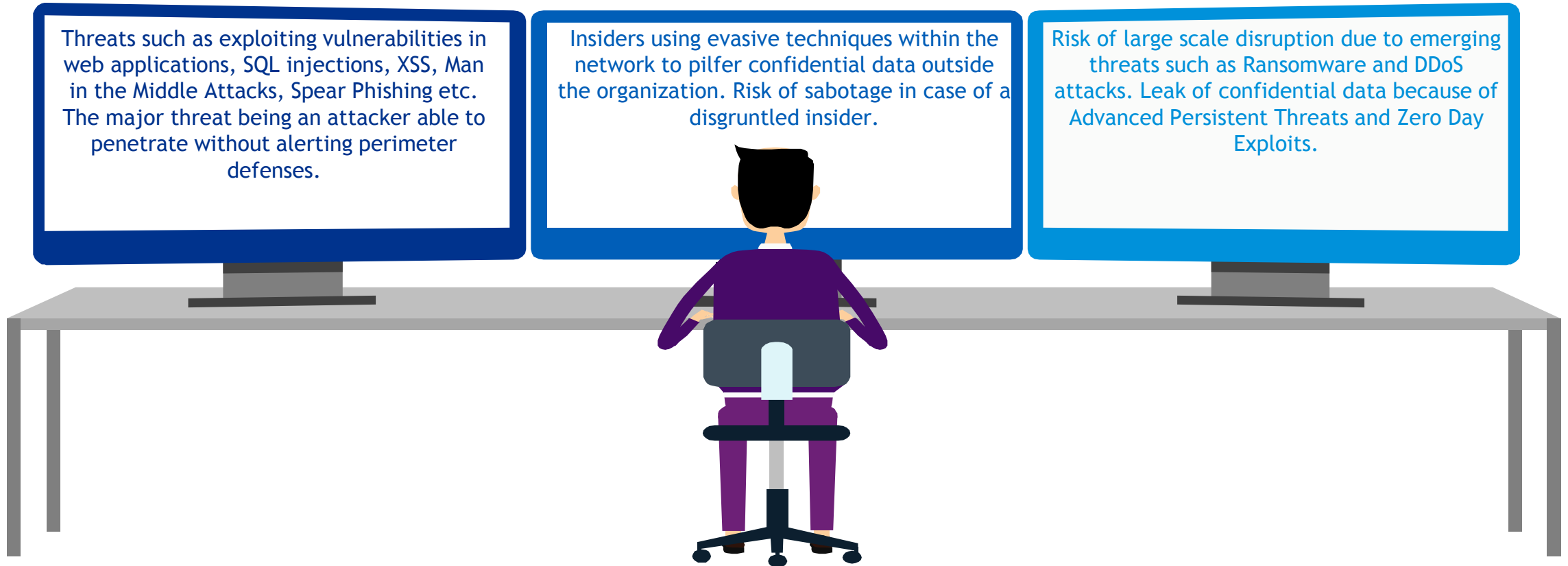
Threats such as exploiting vulnerabilities in web applications, SQL injections, XSS, Man in the Middle Attacks, Spear Phishing etc. The major threat being an attacker able to penetrate without alerting perimeter defenses.

Insider Threats

Insiders using evasive techniques within the network to pilfer confidential data outside the organization. Risk of sabotage in case of a disgruntled insider.

New Age Cyber Threats

Risk of large scale disruption due to emerging threats such as Ransomware and DDoS attacks. Leak of confidential data because of Advanced Persistent Threats and Zero Day Exploits.



*“Establish the need for not just **Sustainable** but **Safe Smart Cities**”*



// Security across smart city ecosystem is as strong as weakest link //

The pervasive impact of Cyber Attacks on Smart Cities

December 23, 2015 – Ukraine Power Grid

Attackers compromised three energy distribution companies systems, affecting 30 substations and leaving 230,000 people without electricity.



March 2016, Kemuri Water Company

Attackers changed the levels of chemicals used to treat water, and the data of 2.5 million utility customers was compromised.



November 4, 2016 – Sweden Air Traffic Control systems

Cyber attack on air traffic control and monitoring system, leading to screen blackout for air traffic controllers and cancellation of several flights



November 25, 2016 – San Francisco Municipal Railway

Ransomware attack on systems



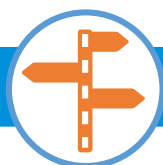
October 7, 2017 – Dallas

Attackers activated 156 emergency sirens around midnight, leading to public chaos and thousand of calls to 911 helpline



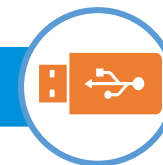
July, 2018 – Department of Homeland Security, US

Russian hackers compromised the networks of multiple U.S. electric utilities and put attackers in a position where they could have caused blackouts



March 22, 2018 – Atlanta Municipal Systems

Ransomware attack on city systems, leading to outage across various city systems



November 18, 2017 – Scaramento Regional Transit Systems

Ransomware attack deleted 30 million files



October 11, 2017 – Sweden Transport Administration Systems

Distributed Denial of Service (DDoS) affected system to monitor trains, road traffic leading to traffic chaos and delays

Cyber Security Pitfalls...





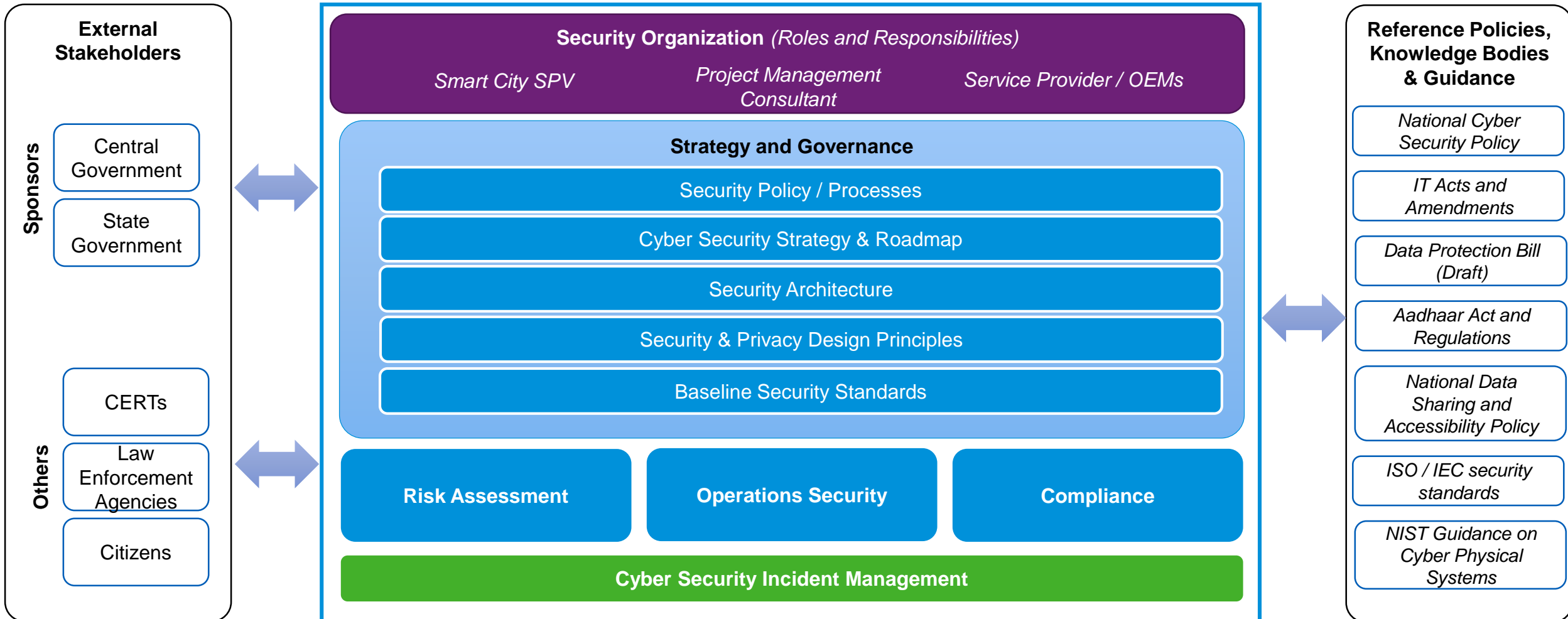
//

Security of Data collected in huge Volumes, Variety and Velocity is imperative for confidence in utilization of smart city services

//

Suggested Framework for Securing Smart Cities

Smart City Cyber Security Framework





// Tech experts debate on 'Security' and 'Privacy', but it is important to build 'Trust' in Smart City Ecosystem //

In Conclusion

1

Establish a formal cybersecurity framework: *A formal guidance based on a well-defined cybersecurity policy and a structured security organisation with clearly defined roles and responsibilities will be really important for governing the cybersecurity posture and reducing the cyber risks*

2

Security must be built-in from the ground up: *Stakeholders and users in smart cities ecosystem will expect security to be built into the system; technology architects should follow an 'always-on' principle that provides high levels of control with appropriate fail-safes.*

3

Security should be deployed in integrated form across value chain: *Smart cities should carefully evaluate their third party suppliers, identify qualified partners, and invest in integrating security, privacy and trust across the ecosystem.*

4

Establish cyber resilient and trusted environment: *Resilience and trust will be established through validation of cyber practices, ensuring compliance and consistent engagement with smart city stakeholders and citizens. This will enhance cyber confidence of citizens and stakeholders on smart city functioning.*

5

Engage across industry, knowledge bodies and regulatory groups to standardise security measures: *Collaboration will reduce ambiguity and accelerate the ability to implement secure products and services within sustainable smart cities ecosystem.*



Thank You!!



kpmg.com/cn/socialmedia

© 2019 KPMG, an Indian Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.