KPMG

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

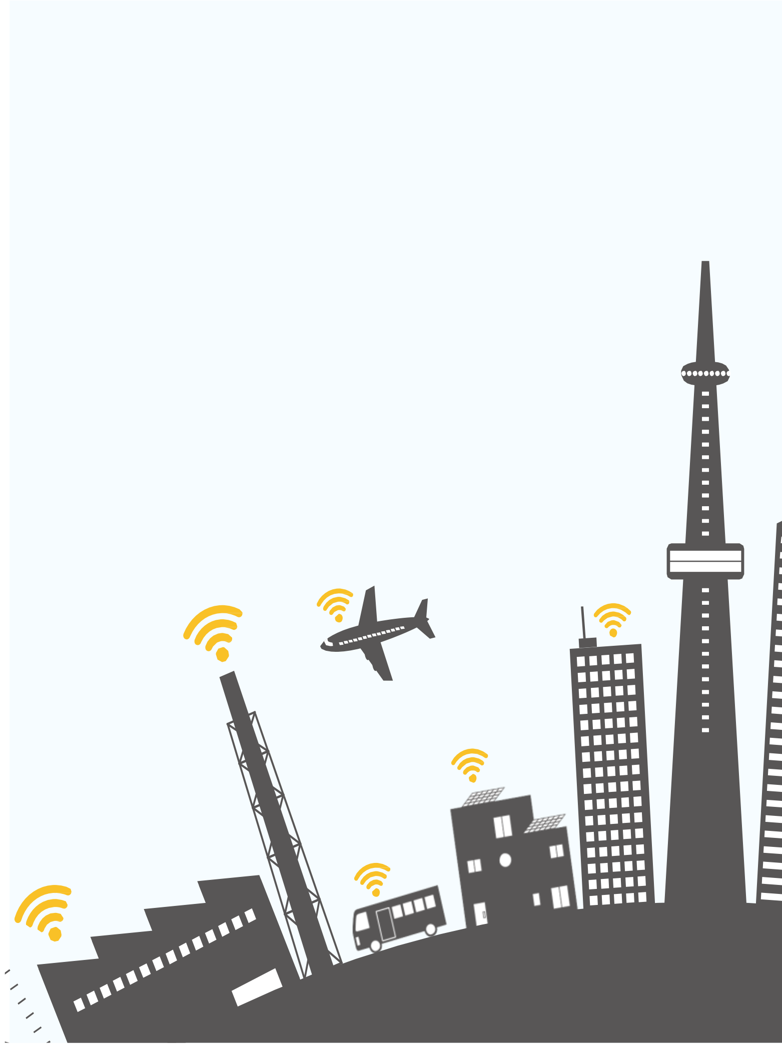
There are 21 mega cities with over 10 million people…

…by year 2025 there will be 30+ mega cities

80% of economic growth will occur in cities…

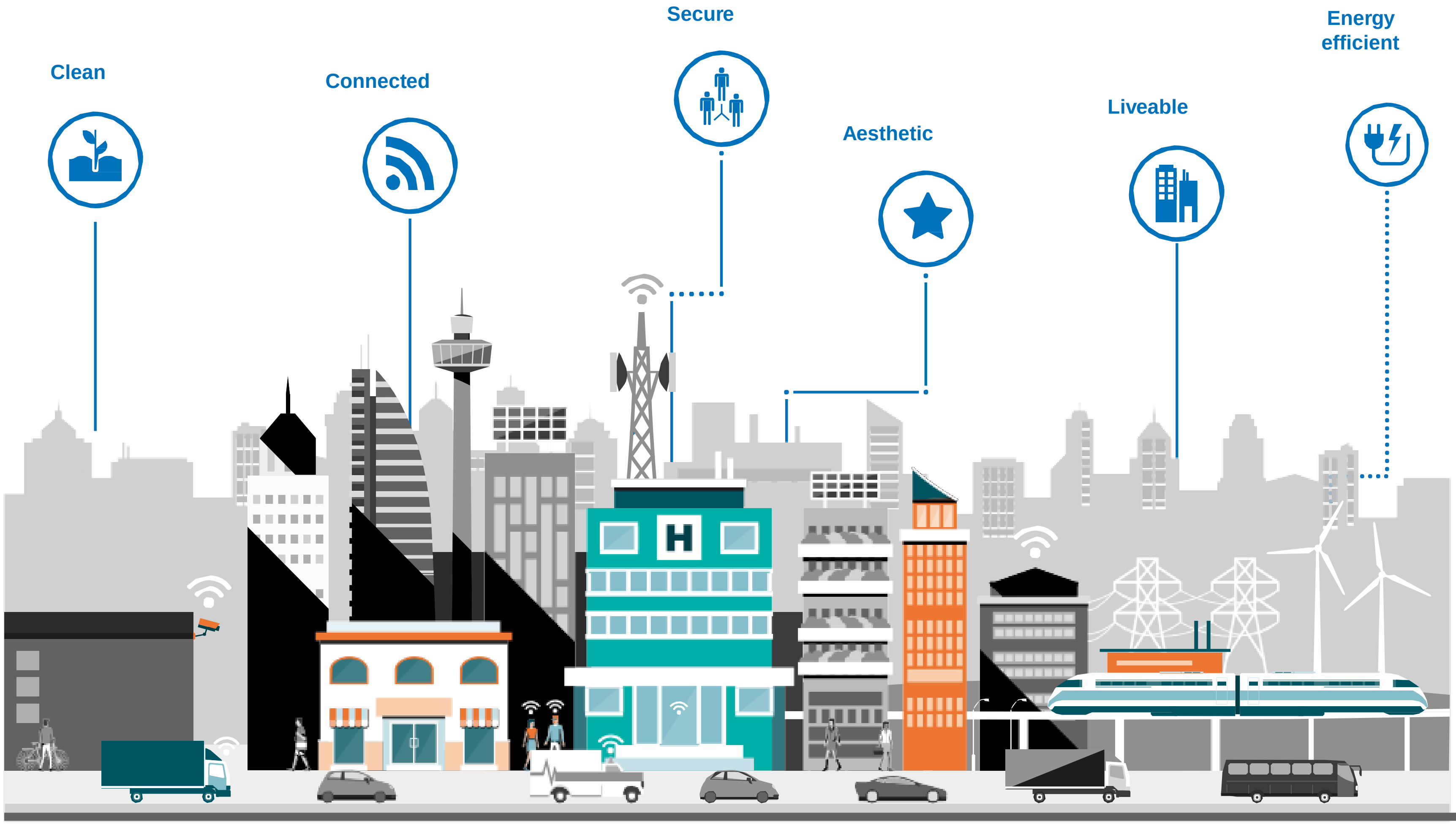
…consuming 60-80% of worlds annual energy needs

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



1 Mobilised

2 Monitored

3 Managed

4 Measured

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
- SLA's 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

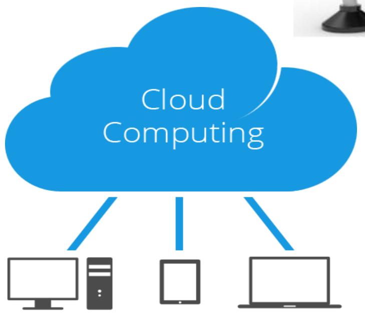
- Personalised education and online training programs
- e-career portals

Anchored on Technology

New technology

code
plan
build
Dev
test
release
deploy
Ops
Operate
monitor

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

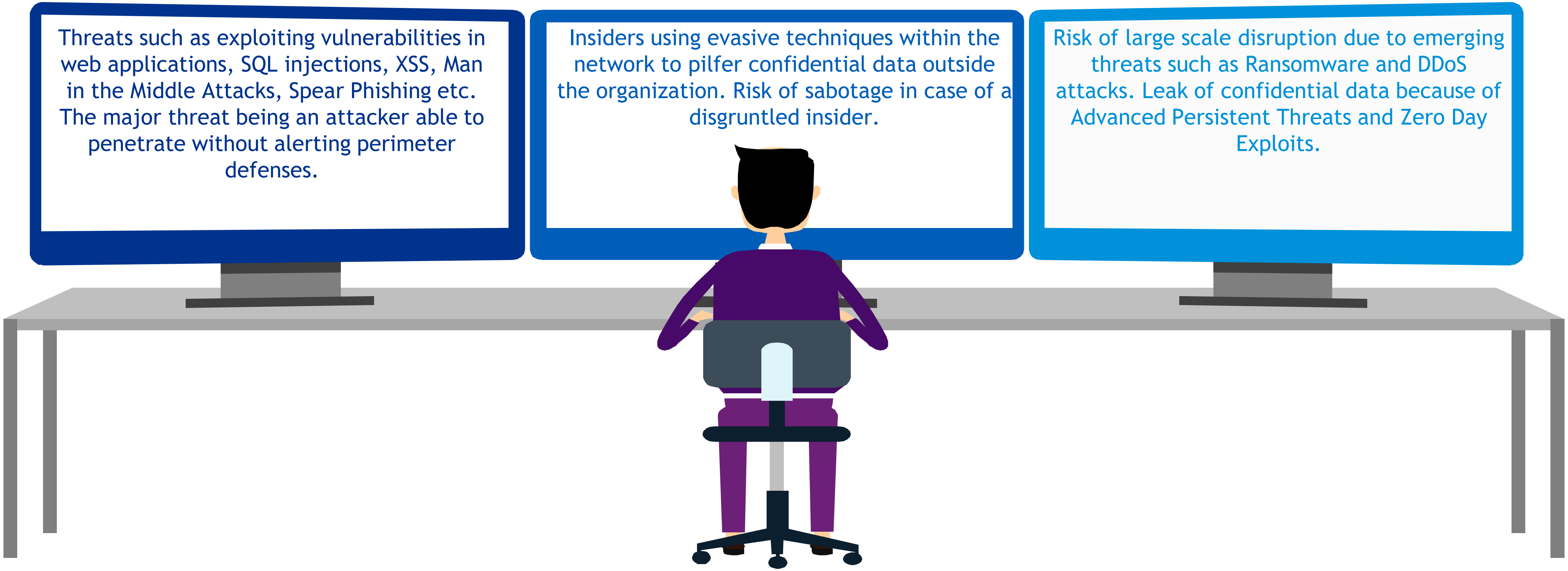


And the associated cyber risks

Traditional Security Threats

Insider Threats

New Age Cyber 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.

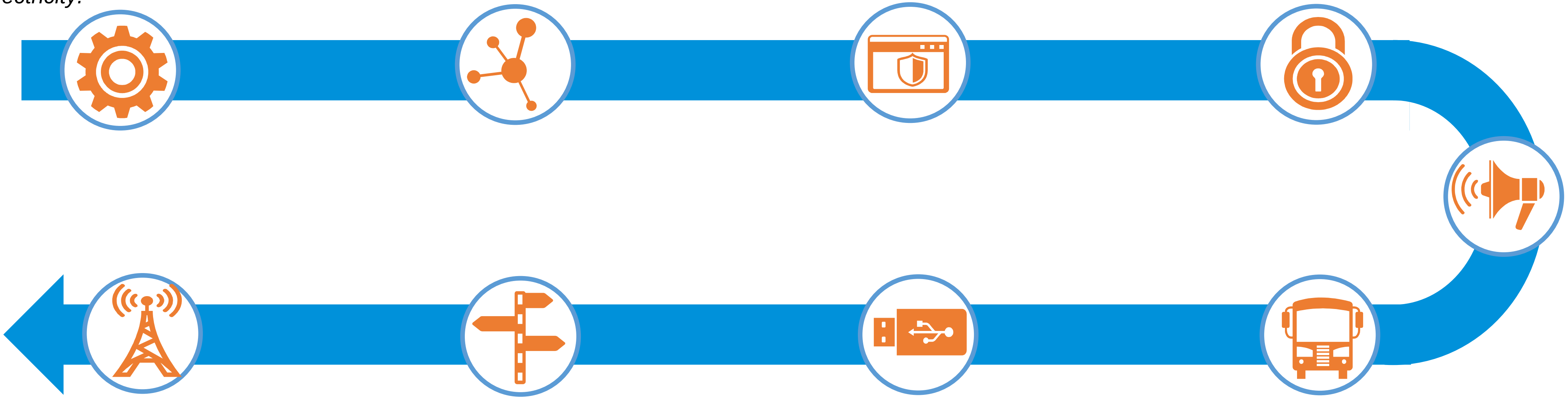
Insiders using evasive techniques within the network to pilfer confidential data outside the organization. Risk of sabotage in case of a disgruntled insider.

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

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

November 18, 2017 – Scaramento Regional Transit Systems
Ransomware attack deleted 30 million files

March 22, 2018 – Atlanta Municipal Systems
Ransomware attack on city systems, leading to outage across various city systems

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

Cyber Security Pitfalls…

01 Inadequate security organization and governance structure to manage security.

02 Inadequate security requirements planning and design of security architecture

03 Increased attack surface due to lack of security standards across smart / connected devices

04 Inadequate and infrequent security assessment of technology assets and infrastructure

05 Lack of identification of Crown Jewels and sensitive data impacting privacy breaches

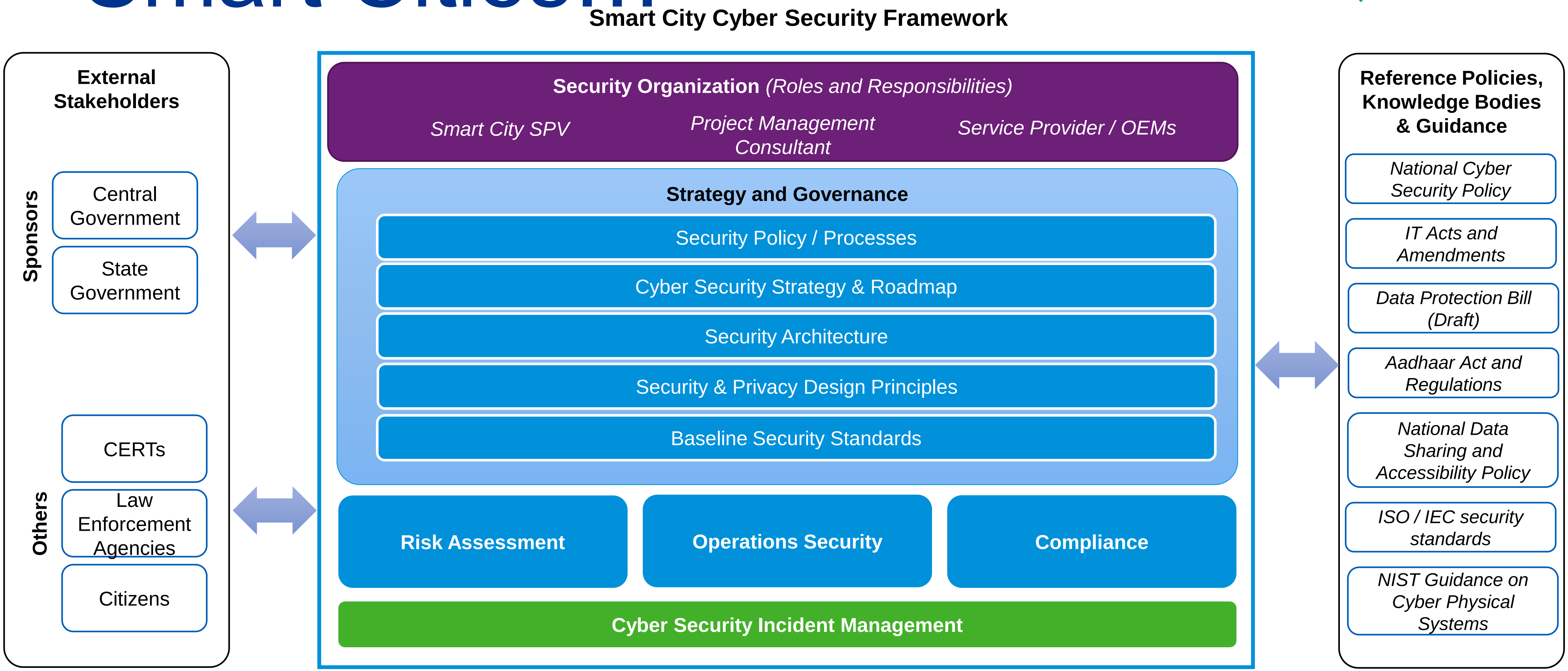
06 Inadequate security monitoring and cyber incident response capability to identify and respond to cyber attacks

"

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
External Stakeholders
Sponsors
Central Government
State Government
Others
CERTs
Law Enforcement Agencies
Citizens
Security Organization (Roles and Responsibilities)
Smart City SPV
Project Management Consultant
Service Provider / OEMs
Strategy and Governance
Security Policy / Processes
Cyber Security Strategy & Roadmap
Security Architecture
Security & Privacy Design Principles
Baseline Security Standards
Risk Assessment
Operations Security
Compliance
Cyber Security Incident Management
Reference Policies, Knowledge Bodies & Guidance
National Cyber Security Policy
IT Acts and Amendments
Data Protection Bill (Draft)
Aadhaar Act and Regulations
National Data Sharing and Accessibility Policy
ISO / IEC security standards
NIST Guidance on Cyber Physical Systems

> "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.*

KPMG

Thank You!!

kpmg.com/cn/socialmedia