DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

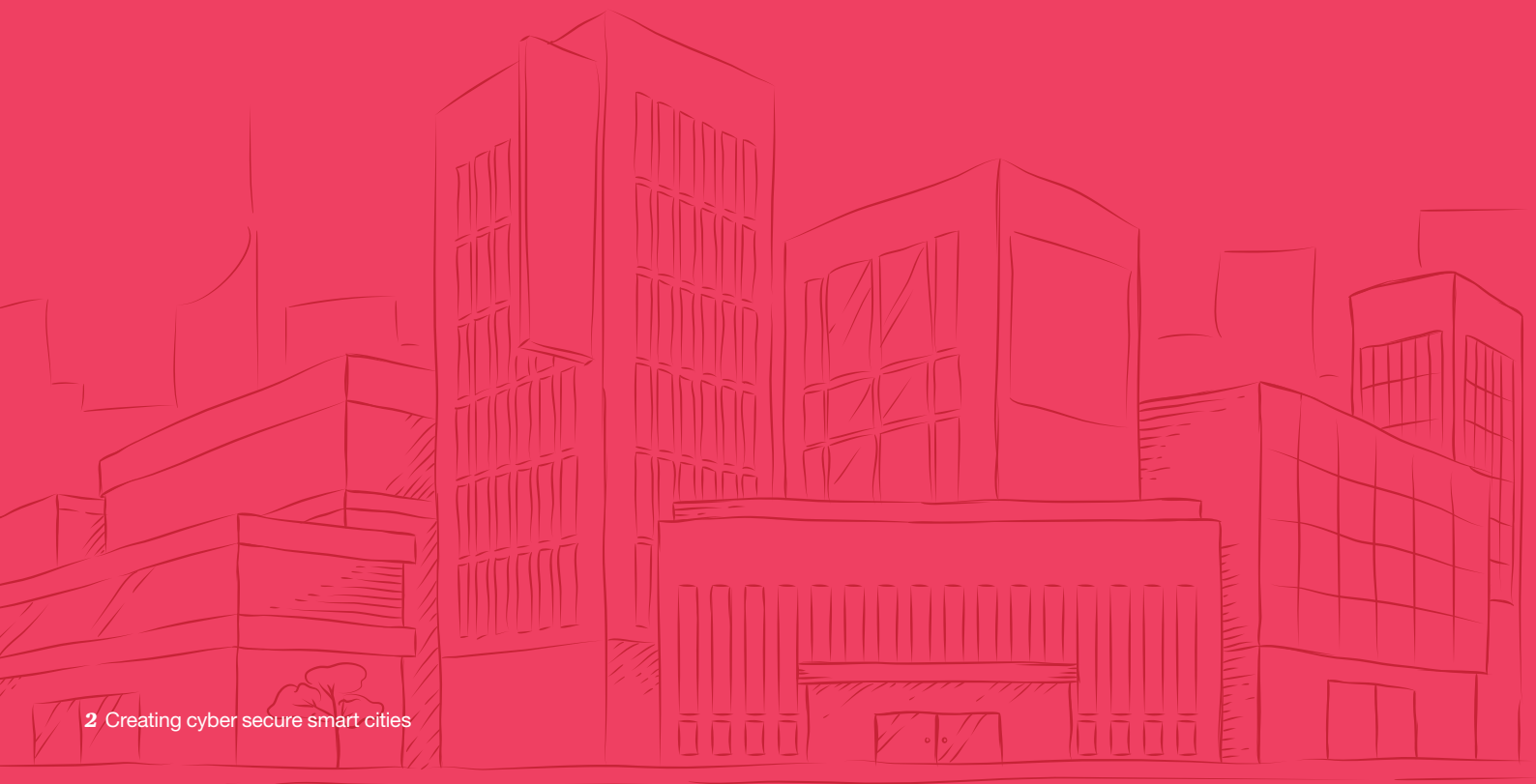
# *Creating cyber secure smart cities*

pwc

*www.pwc.in*

# Contents





# Foreword from the Ministry of Housing and Urban Affairs

**Kunal Kumar**
Joint Secretary,
Mission Director – Smart Cities,
Ministry of Housing and Urban Affairs,
Government of India

India is the fastest growing trillion-dollar economy in the world. The long-term growth prospects of the Indian economy are largely due to its young population, technological progress, and increasing urbanisation. The country is in the midst of a massive wave of urbanisation as millions of people move into towns and cities each year. Enormous investments are being made to meet soaring aspirations and to make towns and cities more liveable.

One such initiative in this direction is India's Smart Cities Mission. The Hon'ble Prime Minister, Shri Narendra Modi, launched the Smart Cities Mission in the year 2015 as an innovative and visionary undertaking towards improving the quality of life and attracting people and investment, setting in motion a virtuous cycle of growth and development. The Smart Cities Mission is expected to drive economic growth and improve the quality of life of people by enabling local development and harnessing technology to create smart outcomes for citizens.

Though the beginning has been excellent, the Smart Cities Mission is still very much a work in progress. There are various economic, technical, and managerial challenges to overcome in mission implementation. One of the most prominent challenges is definitely the cyber security of the smart cities. Considering the ever-expanding risk landscape, India's developing smart cities could be the target for various adversarial interests. From e-governance services to telemedicine and other smart city services – the acceptance and delivery of all of these services depend on the security of the underlying technology powering them. This needs collective effort from every stakeholder associated with the smart city ecosystem.

As we discuss the right mechanism to deal with this rising threat, it must also to be recognised that there are multiple stakeholders in the smart city environment. Hence, we should strive to develop a holistic mindset towards cyber security challenges that takes into account the requirements of all stakeholders involved. It evidently becomes very important to secure India's smart cities as they impact the lives of millions of residents.

The Ministry of Housing and Urban Affairs (MoHUA) has already taken initiatives in terms of creating the cyber security model framework for smart cities. However, a concentrated and coordinated effort from all the stakeholders involved is critical.

# Foreword from Data Security Council of India

**Rama Vedashree**
Chief Executive Officer
Data Security Council of India

India's digitalisation roadmap is expected to catapult its digital economy to 1 trillion USD by 2025. India is witnessing an unforeseen digital transformation, and at the same time, a rapid rate of urbanisation. The Government of India's 100 Smart Cities Mission blends these digitalisation and urbanisation waves, and endeavours to accomplish urban renewal through a Pan-City Smart Solutions initiative, and technology-enabled 'city improvement (retrofitting), city renewal (redevelopment) and city extension (greenfield development)'.

While the smart city initiative focuses on sustainable development of our cities and harnessing digital technologies for integrated citizen service delivery, it demands a strong focus on cyber security. It is imperative for stakeholders to review and make efforts towards ensuring the safety, security and privacy of citizens and enhancing our cities' capability to mitigate cyber security risks.

Globally, countries have deployed technologies and controls to avoid loss of data, network lockdowns, and stalling of critical services that can otherwise cripple a city's functioning. We also need to take appropriate measures to create cyber secure smart cities that can minimise attacks and potential risk to our city infrastructure and services. Recognising cyber security as a key priority, the Ministry of Housing and Urban Affairs (MoHUA) published the 'Cyber Security Framework for Smart Cities' on 20 May 2016 and issued an advisory to all smart cities to drive conformance to this framework.

This report on 'Creating cyber secure smart cities', jointly developed by DSCI and PwC, is an attempt to reinforce the attention that smart city administrators need to give to cyber security in all their projects as they infuse smart solutions. With a fine blend of global and Indian instances, this report serves as a preliminary guide for smart city stakeholders to understand the risks and steps that need to be taken to enhance the cyber security posture of smart cities. The report acknowledges that cyber security is the combined responsibility of various stakeholders—MoHUA at the central level; and smart city special purpose vehicles (SPVs), project management consultants (PMCs), master system integrators (MSIs), original equipment manufacturers (OEMs), third-party vendors, among others, at the smart city level.

Finally, we have provided guidance to the various stakeholders across the smart city planning, design/implementation and operations phase. We do hope that this report serves as a helpful guide in strengthening the cyber security posture of smart cities and in driving stakeholder collaboration.

# Message from PwC

**Sivarama Krishnan**
Leader, Cyber Security
PwC India

As India's population gradually shifts to urban areas, there is no better solution to manage the shift than the Smart Cities Mission. It is a step in the right direction that will help create an ecosystem conducive to sustaining a larger mass even with limited resources. Digital technology, which is at the heart of this mission, is going to propel smart cities. However, the adoption of technology throws up its own set of challenges – for example, cyberattacks and the risk of privacy violation. We need to understand that the use of technology in a city-like set-up automatically widens the threat surface. Devices and machines, interconnected over the network and installed to generate and exchange an enormous amount of data, enable smart services. However, these smart services attract undesired attention from miscreants and hackers who can disrupt their provision. By exploiting loose or inappropriately secured endpoints, they can gain easy and privileged access to major control systems.

India cannot afford to have inadequately secured smart cities. Cyber security needs to be ingrained in the systems right from the beginning or during the implementation phase. All stakeholders of smart cities, including the government and appointed businesses, must pay heed to the requirements for robust security, and take measures under the concurrent and continuous information security functions: identify, protect, detect, respond and recover.

Although the Government of India looks committed to creating secure and safe smart cities with a host of steps, concerns and challenges related to governance and operations in the wake of attacks and hacking incidents have to be duly addressed. Through this knowledge paper, we want to lay emphasis on the importance of cyber security and the need to evaluate the existing landscape and understand the criticality of taking up India-specific challenges head-on. Our analysis and evaluation of the smart cities project suggests that there is an immediate need to tighten the screws for secure and uninterrupted transmission and flow of information/data over a wide and complex network. Unaddressed vulnerabilities will most likely serve as backdoors for cyber intruders.

We have prescribed action items to assist different smart city stakeholders and create a strategy for cyber security implementation and oversight. A well-coordinated and direct approach is recommended, must be adopted and worked upon. The action items are a result of a careful, exhaustive evaluation of the global best practices for the protection of smart cities and the guidelines of the Indian government. The paper will assist organisations, agencies and governments in India engaged in building strong defences against cyberthreats.

Robust cyber security measures will help citizens repose trust in smart cities.

# *Making smart cities cyber secure*

Urbanisation is a global trend and India is no exception. In India, 31% of the population currently lives in cities. The number continues to grow, with more people migrating to urban areas for better employment opportunities, healthcare and educational facilities, and a higher standard of living.[1] This trend is expected to continue in the coming years, with city population growth projected to reach almost 50% by 2030.[2] The Indian government, having acknowledged this shift, undertook steps to develop 100 smart cities under the Smart Cities Mission launched in the year 2015.[3]

The smart cities leverage technology and utilise existing and planned infrastructure investments to provide a higher quality of living to residents. Smart cities are powered by advanced technologies such as the Internet of things (IoT) and sensors along with the traditional information technology (IT) and operational technology (OT) systems and devices. These advanced and traditional technologies, distributed across the smart city, work in an integrated manner to generate intelligent and actionable information to help in providing services to residents in an efficient and sustainable manner.[4]


1 Census India, 2011: http://censusindia.gov.in/2011-prov-results/paper2/data_files/india/Rural_Urban_2011.pdf

2 https://www.thehindubusinessline.com/economy/policy/half-of-indias-population-will-be-living-in-urban-areas-by-2030-says-puri/article9891352.ece

3 http://smartcities.gov.in/

4 http://smartcities.gov.in/content/

### Intelligent traffic management system (ITMS)

The ITMS includes automating the process of traffic management by optimally configuring traffic junction signals on real-time basis.

### Closed circuit TV (CCTV) surveillance

The city surveillance system comprises video and audio surveillance that converge onto possible crime vectors and their prevention.

### Smart water management

The smart water management system gathers meaningful and actionable data about the flow, pressure and distribution of a city's water and streamlines the processes.

### Automatic fare collection system

This system includes an automatic gate machine, ticket vending machine and ticket checking, along with analysis of passenger flow.

### Smart poles

Smart poles combine the benefits of LED lighting, Wi-Fi connections and mobile connectivity in an integrated manner.

### E-governance

E-governance is the use of information and communication technology (ICT) to provide public services to citizens, by re-engineering internal business processes and increasing the transparency and accountability of government schemes.

### Smart waste management

This includes a web-based tracking and monitoring system pertaining to functions like recycling, reusage and disposal.

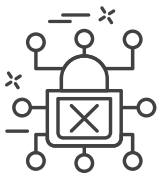
### Telemedicine

Telemedicine provides digital channels to consult physicians and avail medical guidance remotely, including requesting emergency services and medical facilities.

### Enterprise GIS application

It is an integrated cross-sectoral platform to collect, manage, compile, analyse and visualise spatio-temporal information for sustainable urban planning, development and management.

Though integrated technologies assist in efficient delivery of services, using them expands the threat landscape. Cyberattacks, which earlier targeted data centres, are now directed towards numerous systems and devices spread across a smart city. This enhanced threat surface provides huge opportunities for hackers to launch attacks. A single intrusion by them may leave the entire smart city network compromised. Cyber security has always been a pain point for organisations. With the increased threat surface, it will be prudent for smart cities to focus on cyber security to be able to deliver a safe and secure environment to citizens.



***With 100 smart cities, India has an aggressive agenda of socioeconomic development. Though the technologies utilised in smart cities promise an improved quality of life, they also expand the threat landscape. This phenomenon has also been observed across the globe, wherein many cities were compromised and services were brought to halt.***

# *Global smart cities targeted by adversaries*

There's no denying that smart cities have paved the way for a better and healthy life. However, they have their own pitfalls. On the one hand, this has led to new socioeconomic opportunities; on the other, smart cities have opened up new avenues for attackers who can indulge in disruption and carry out criminal activities. Many smart cities across the globe have faced major cyberattacks in the past few years. With the passage of time, attacks have grown in sophistication and severity, resulting in cities coming to a standstill.

### Atlanta smart city network locked down

Attackers encrypted files, locking employees out of the smart city network completely, while the rest were forced to shut down to prevent the virus from spreading. It is believed that the cyberattack destroyed 'years' worth of police dash cam video footage.[5]

### Emergency sirens activated, resulting in widespread panic in Dallas

Attackers activated 156 emergency sirens at 11:40 p.m., waking up and frightening a lot of people until 1:20 a.m., when the alarms were turned off.[6]

### Massive power outage in Ukraine, leading to blackouts

BlackEnergy malware was planted within the networks of multiple regional power companies in Ukraine and the technical support phone lines of targeted firms were also flooded, which led to blackouts in different regions in Ukraine[7].

### Sensitive health data of 1.5 million patients, including Prime Minister's, stolen in Singapore

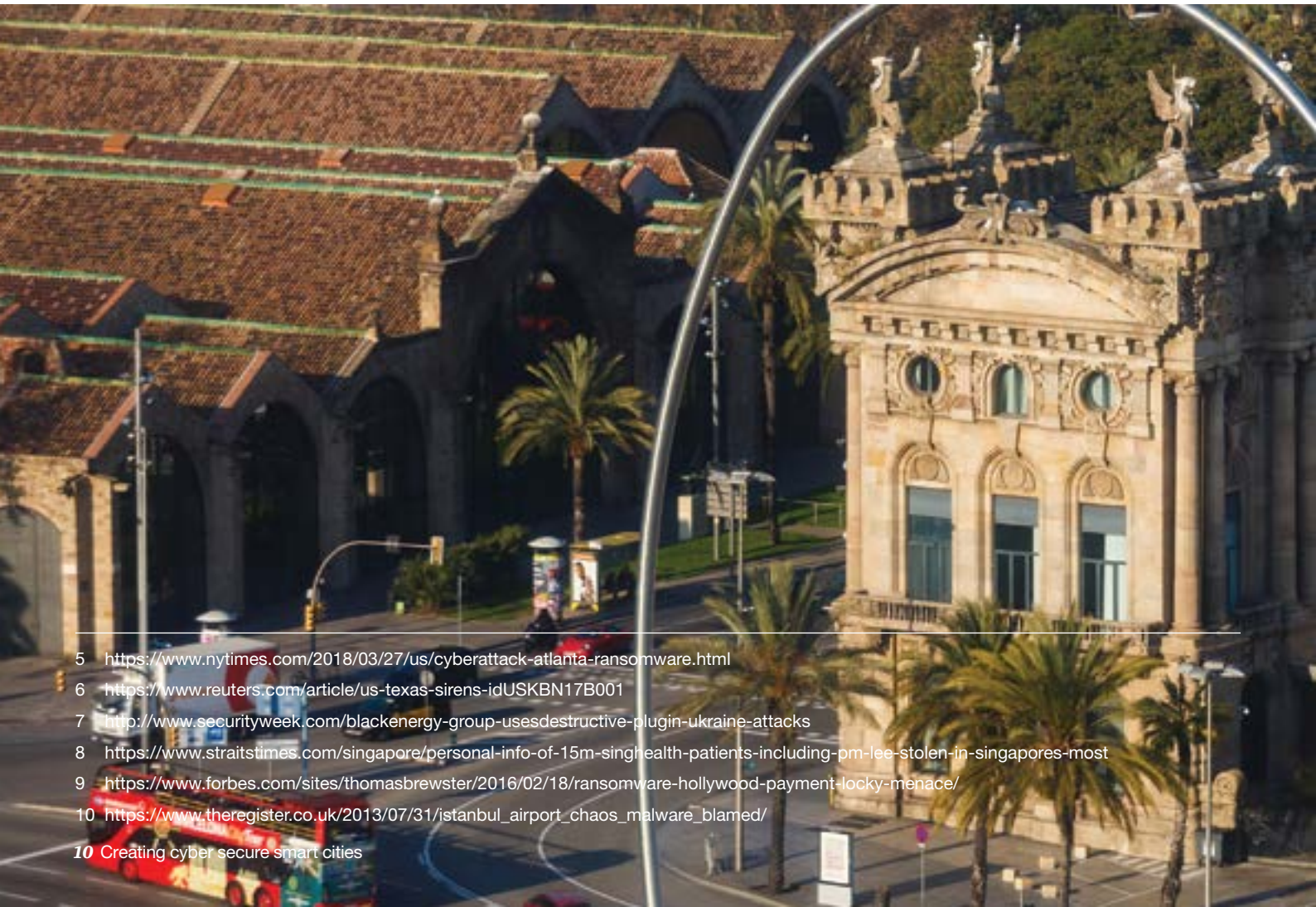
Hackers targeted Singapore's largest healthcare institution, SingHealth, and stole the personal profiles of 1.5 million patients along with the details of prescriptions for 1,60,000 others.[8]

### California hospital remained shut for a week, paid a ransom in order to resume operations

A hospital in California had to shut down all its systems for a week as it was attacked by cybercriminals demanding a ransom in bitcoins.[9]

### Airport operations impacted, causing significant delays in Istanbul

The airport passport system was infected using malware and several flights were delayed due to the unavailability of the passport system.[10]



5 https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html
6 https://www.reuters.com/article/us-texas-sirens-idUSKBN17B001
7 http://www.securityweek.com/blackenergy-group-usesdestructive-plugin-ukraine-attacks
8 https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most
9 https://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/
10 https://www.theregister.co.uk/2013/07/31/istanbul_airport_chaos_malware_blamed/

## Hacking attack caused 'massive damage' at German steel works

A blast furnace at a German steel mill caused massive damage following a cyberattack on the plant's network. It is believed that attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.[11]

## Estonia faced a full-scale cyberwar

Estonia was subjected to cyberterrorism in which the attackers penetrated and brought down key government websites, rendering them redundant. A number of techniques such as ping floods and botnets were deployed for the penetration process.[12]

## Pornographic clip played on advertisement display at a metro station in New Delhi

Miscreants played a pornographic video on an advertisement screen installed at a metro station in New Delhi and the entire sequence was shot by a few commuters on their mobile phones, after which the incident went viral on social media. It is believed that the LED TV system was under commissioning and the Wi-Fi port was accessible due to lack of password controls.

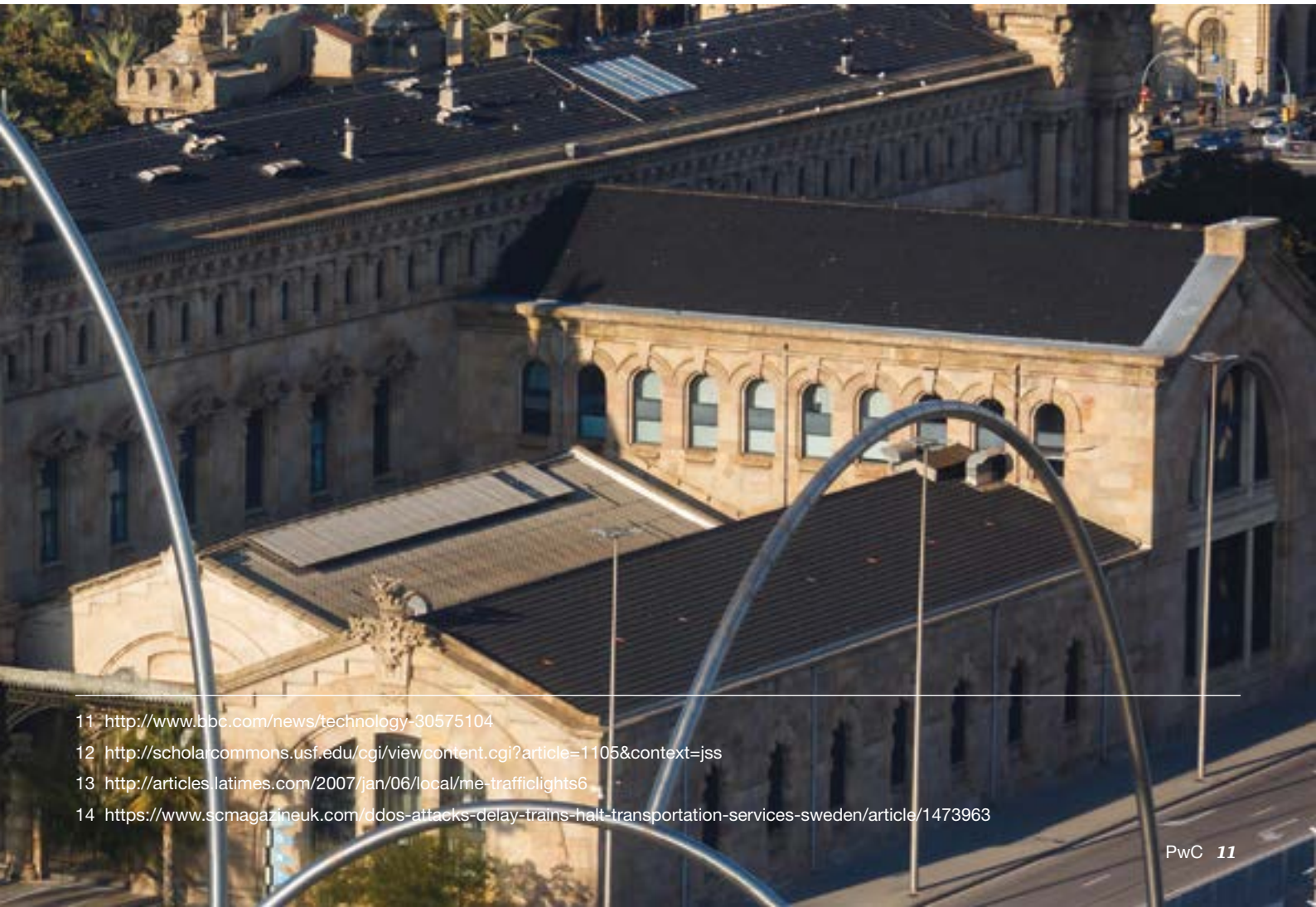
## Sabotage of traffic signals in Los Angeles

Two traffic signal engineers hacked into the systems and tweaked the timings of the signals at four critical intersections, causing havoc within the city.[13]

## Distributed Denial of Service (DDoS) attacks delay trains in Sweden

A series of DDoS attacks aimed at Sweden's transportation services caused train delays and disrupted travel service.[14]

***From loss of health data to complete network lockdown, global smart cities face the continuous onslaught of cyber security breaches. While these attacks have attempted to cripple smart cities, they also provide an opportunity to the various countries to learn from such incidents and appropriately build security controls to safeguard against them.***



11 http://www.bbc.com/news/technology-30575104

12 http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

13 http://articles.latimes.com/2007/jan/06/local/me-trafficlights6

14 https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963

# *Key cyber security initiatives taken across the globe*

Worldwide, countries acknowledge the threats their smart cities face from cybercriminals, and have accordingly invested in ramping up the security and privacy layers around their infrastructure and data. Many countries have set a precedent by taking significant steps on regulations, standards and framework to fortify cyber security.

## 1 United Stated of America (USA)

a. **Internet of Things Cyber Security Improvement Act, 2017:** The USA government released the Internet of Things Cyber Security Improvement Act, 2017, to establish minimum cyber security standards for IoT devices.[15]

b. **Cyber Physical Systems (CPS) Framework 1.0:** The National Institute of Standards and Technology's CPS Public Working Group (PWG) released the CPS PWG Cyber Physical Systems Framework 1.0, detailing the cyber security privacy and strategy for the common elements—identification, implementation and monitoring of cyber security services of the CPS.[16]

c. **Cyber Security Guidelines for Securing Smart Cities:** Multiple cyber security vendor firms collaborated to launch a not-for-profit forum 'Securing Smart Cities', which released 'Cyber Security Guidelines for Smart City Technology Adoption'.[17]

d. **NYC Secure Initiative:** NYC Secure is an initiative for citizens of New York City. It includes a free city-sponsored smartphone protection app that will issue warnings to users when suspicious activity is detected on their phones, as well as new protection for the city's public Wi-Fi networks.[18]

e. **National Infrastructure Protection Plan (NIPP 2013) – Partnering for Critical Infrastructure Security and Resilience:** It outlines the plan for collaboration amongst the government and private sector participants to manage risks and achieve cyber resilience.[19]

f. **City-Based Cyber Lab:** Los Angeles launched a City-Based Cyber Lab to strengthen cyber security for its businesses and residents. The lab is a public-private partnership that will disseminate information and intelligence based on analysis of more than one billion security-related events and over four million attempted intrusions into city networks per day.[20]

## 2 Europe

a. **European Union (EU) Network and Information Security (NIS) Directive for Sectoral Supervision:** The EU released the NIS directive which clearly indicated that the member states needed to supervise the cyber security of critical market operators in the country.[21]

b. **Certification Framework for Devices:** This framework seeks to ensure an EU-wide certification scheme consisting of comprehensive rules, technical requirements, standards and procedures. This will be based on agreement at the EU level on the evaluation of the security properties of a specific ICT-based product or service.[22]

c. **Baselines Security Recommendations for IoT:** The EU provided 'Baseline Security Recommendations for IoT' detailing the critical attack scenarios, need for security by design and the security gaps in the IoT ecosystem, followed by recommendations.[23]

d. **European Union Agency for Network and Information Security (ENISA) Guidelines for Cyber Security of Smart Cities:** ENISA has released two detailed guidelines for cyber security of smart cities—architecture model for public transport, and security and resilience for smart health service and infrastructure.[24]

e. **Critical Infrastructure Security Analysis (CRISALIS) Programme:** The CRISALIS programme is aimed at providing means to secure critical infrastructure environments from attacks caused by malware and threat agents such as Stuxnet and Duqu.[25]

15 https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

16 https://pages.nist.gov/cpspwg/

17 https://securingsmartcities.org/wp-content/uploads/2016/03/Guidlines_for_Safe_Smart_Cities-1.pdf

18 https://secure.nyc/

19 https://www.dhs.gov/national-infrastructure-protection-plan

20 https://www.lacity.org/blog/mayor-garcetti-launches-nations-first-city-based-cyber-lab

21 https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive

22 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

23 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

24 https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-infrastructure?tab=publications

25 ct.eu/node/38

## 3 Singapore

a. **Singapore Cybersecurity Act, 2018:** The act establishes a legal framework for the oversight and maintenance of national cyber security in Singapore with the objective of strengthening the protection of critical information infrastructure (CII), preventing and responding to cyber security threats and incidents, sharing cyber security information and establishing a light-touch licensing framework for cyber security service providers.[26]

b. **Personal Data Protection Act (PDPA), 2012:** The PDPA establishes a data protection law that comprises various rules governing the collection, storage, use, disclosure and care of personal data. A Personal Data Protection Commission (PDPC) is also defined which ensures the enforcement of the act.[27]

c. **Internet of Things (IoT) Ecosystem Standards:** The Internet of Things Technical Committee (IoTTC) focuses on the standardisation needs in IoT technologies, such as sensor networks, system interfaces, data management and security. Thus far, four technical standards on IoT have been published.[28]

d. **National Cybersecurity Research & Development Lab:** It was set up with the primary aim of maintaining a shared national infrastructure that provides computing and networking resources for cyber security research and development.[29]

e. **Cyber Security Start-up Hub:** Singapore opened its first cyber security entrepreneur hub called ICE71 'Innovation Cybersecurity Ecosystem at Block 71' to strengthen its growing cyber security ecosystem by attracting and developing competencies and deep technologies.[30]

## 4 Australia

a. **Internet of Things (IoT) Alliance Australia:** The IoT Alliance Australia (IoTAA) works with the objective of accelerating IoT innovation and adoption in Australia. Recently, they launched a report, 'Enabling the Internet of things for Australia', detailing the need for privacy by design, data protection and testing of IoT devices in the area of smart cities, health, energy, etc.[31]

b. **Guidelines & Best Practices in Smart Cities:** In 2018, the Smart Cities Council Australia and New Zealand released a best practices guide covering the cyber security standards in 2018.[32]

c. **Critical Infrastructure Program for Modelling and Analysis (CIPMA):** It was launched to assist critical infrastructure owners and operators in understanding network interdependencies and improving resilience by developing and using the tools of modelling and simulation to provide impartial, evidence-based and objective analysis of potential natural or human-induced disruptions to critical infrastructure.[33]

d. **The Trusted Information Sharing Network (TISN):** It is Australia's primary national engagement mechanism for business-government information sharing and resilience-building initiatives on critical infrastructure resilience and cyber security.[34]

26 hhttps://www.csa.gov.sg/legislation/cybersecurity-act

27 https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

28 https://www.imda.gov.sg/itsc/technical-committees/internet-of-things-technical-committee-iottc

29 https://ncl.sg/about

30 https://ice71.sg/

31 https://www.iot.org.au/about/

32 https://anz.smartcitiescouncil.com/system/tdf/anz_smartcitiescouncil_com/public_resources/smart_cities_standards_best_practice_guide_issue.pdf?file=1&type=node&id=5297

33 https://www.tisn.gov.au/Documents/CIPMA-flyer.PDF

34 https://www.tisn.gov.au/Pages/default.aspx

## Learnings from global initiatives

**Effective regulations**

Cyber security and privacy acts have been introduced to ensure security is given the foremost importance. Existing regulations have been updated at periodic intervals to incorporate the smart city security perspective.

**Framework and standards for ecosystem**

Several countries across the globe have established cyber security frameworks and defined security and privacy guidelines in the context of smart cities. Baseline security standards and guidelines have also been introduced for different stakeholders.

**Collaboration and capacity development**

Cyber security information sharing platforms have been created for collaboration across sectors, including smart cities, finance and energy. A number of programmes have been launched globally for building skills and capabilities in cyber security. A conducive environment has also been set up to promote cyber start-up hubs.

***Globally, smart cities have launched numerous cyber security initiatives spread across three pillars—effective regulations, framework and standards for the ecosystem, and collaboration and capacity building. India is following in their footsteps.***

# *India has just begun the journey to secure smart cities*

India's efforts to protect its smart cities are timely. A host of policies and regulations have been designed to protect the smart city infrastructure from cyberattacks. Some of the existing/upcoming regulations on security and privacy are also applicable to smart cities, thereby helping to build secure cities.

## India

a. **Ministry of Housing and Urban Affairs (MoHUA) Guidelines:**[35] MoHUA, the Government of India, released a model framework for cyber security in smart cities on 20 May, 2016. It covers the security of smart cities across different layers, namely sensor layer, communication layer, data layer and application layer. The major guidelines include, but are not limited to:

- Designing a secure network architecture based on the National Institute of Standards & Technology (NIST) reference IT architecture
- Security solutions that needs to be considered while developing a smart city
- Secure storage and transmission of data between different systems and devices implemented in the smart city
- Security assessment of the services before and after going live
- Compliance with standards such as ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180, BSI PAS 182, Protected Extensible Authentication protocol (PEAP) and 3rd generation Partnership Project (3GPP), as applicable
- Setting up of security monitoring for smart city network, devices and sensors
- Reporting of security incidents to relevant bodies such as Computer Emergency Response Team – India (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC).

b. **The National Critical Information Infrastructure Protection Centre (NCIIPC), 2014:** NCIIPC has been identified as the nodal agency under the National Technical Research Organisation for the protection of critical information infrastructure. The formal roles and responsibilities of the NCIIPC include cooperation strategies, issuing guidelines, advisories and coordination with CERT-In. The NCIIPC has defined controls for the critical infrastructure sectors to enhance security.[36]

c. **National Cyber Security Policy, 2013:** The policy aims to create a secure cyber ecosystem in the country and strengthen the regulatory framework.[37]

d. **Information Technology Act (IT Act), 2000, and its amendments:** The IT Act includes rules on the protection of sensitive personal data or information and provisions for electronic service delivery, publication of content of a specific nature on the Internet, and the penalties applicable in case of any offence.[38]

e. **Aadhaar Act, 2016, and its regulations:** The Aadhaar Act, 2016, defines how Aadhaar-related data is to be captured, stored and processed. Aadhaar data includes not only biometric information (fingerprints, iris and photo) but also the demographic details of the resident. The Aadhaar Act, 2016, forms the basis of various e-governance initiatives such as distribution of services and benefits to residents of India.[39]

f. **Draft Personal Data Protection Bill:** The Personal Data Protection Bill includes provisions to protect personal data as an essential facet of information privacy. The bill provides guidelines on the data processing grounds, rights of the data principal, penalties and exemptions, amongst other areas. The bill aims to protect the autonomy of individuals from data privacy violations by the state and private entities. Once enforced, the bill will impact how the smart city information systems store and process personal/sensitive data.[40]

g. **Draft Digital Information Security in Healthcare Act (DISHA):** The draft DISHA document was recently released in the public domain for comments. It aims to set up a National Health Authority in India which shall be responsible for enforcing privacy and security measures for electronic health data, and to regulate storage and exchange of the same.[41]

35 http://mohua.gov.in/pdf/58fd92b5545b85821b621a862dCyber_Securitypdf.pdf

36 NCIIPC. Retrieved from https://nciipc.gov.in/

37 http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

38 http://meity.gov.in/content/information-technology-act-2000

39 https://uidai.gov.in/legal-framework/acts.html

40 http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

41 https://mohfw.gov.in/newshighlights/comments-draft-digital-information-security-health-care-actdisha

# *Indian smart cities face specific challenges*

Challenges specific to the Indian context weaken the efforts towards cyber security implementation in smart cities. The major challenges have been 1) cyber security not figuring amongst top priorities and 2) limited stakeholder awareness on cyber security. While security should be a prerequisite, in the Indian context, it is often an afterthought. As cities throw their weight behind timelines to implement services, security takes a backseat. Based on our analysis and on-ground assessments, the smart cities today face multiple challenges in implementing cyber security.

**Security governance**

There is no security organisation responsible for ensuring cyber security within smart cities. Additionally, there is no or limited consideration of cyber security during the various phases of smart city development.

**Budget allocation**

Limited budget is allocated for cyber security in the overall smart city budget. Even when a budget is allocated, it does not match the risk profile of smart cities, thereby making the process of setting up adequate defences a difficult proposition.

**Security products selection and implementation**

Business-driven risk assessments are not conducted to identify appropriate security products based on the risk profile of the smart city. Additionally, there are no baseline security guidelines for implementation and configuration of security products.

**Cyber security capability and awareness**

Smart city stakeholders have low awareness of cyber security risks and vulnerabilities. Further, the stakeholders responsible for securing the smart cities, have limited cyber security capabilities.

**Review and monitoring mechanism**

There is no mechanism in place to regularly perform security assessments of the smart city set-up in order to identify and mitigate security risks on a continual basis.

***Indian smart cities are exposed to challenges that hinder the development of secure cities. These challenges leave smart city services prone to serious security vulnerabilities which, if exploited, can paralyse smart city operations or do irreparable damage.***

# *Security risk landscape for Indian smart cities*

The Indian Smart City technology architecture can be understood through the four logical layers: sensor, communication, data and application layers. The technology across these four layers works in an integrated manner to deliver Smart City services.

**Indian smart city ICT architecture**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | E-governance | City surveillance | Smart waste management | Smart poles | Smart water management | Telemedicine | Automatic fare collection | Enterprise GIS application | Intelligent traffic management |
| Application layer | Video management system | | Integrated traffic management system | | Waste management application | | Water management application | | Telemedicine application |
| | Flood monitoring system | | Smart pole application | | Parking management system | | GIS | | Other enterprise applications/APIs |
| Data layer | Master data management | | Citizen personal and health database | | Predictive/prescriptive analytics | | Big data analytics | | |
| | KPI indicators | | Dashboards and reports | | Alerts | | Other advanced analytics | | |
| Communication layer | Ethernet | | Wi-Fi | | GPRS | | Fibre | | |
| | Firewall and security devices | | Routers and switches | | Communication channels | | Other network and communication devices | | |
| Sensor layer | Surveillance cameras | Environmental and seismic sensors | | Parking sensors | | Water level detection | | Traffic detection system | Speed detection cameras |
| | Audio detection sensors | RFID tags | Smoke detection | | Leakage detection | | Readers | Smart meters | Red-light violation detection |

Our analysis and on-ground assessment of a few smart cities suggest that the technology powering the Indian smart city services are very much prone to vulnerabilities, which can lead to potential social, health, economic and/or reputational risks.
The presence of inherent challenges, lack of granular guidelines and regulations, and India-specific issues add to the complexity of the risk landscape for Indian smart cities.

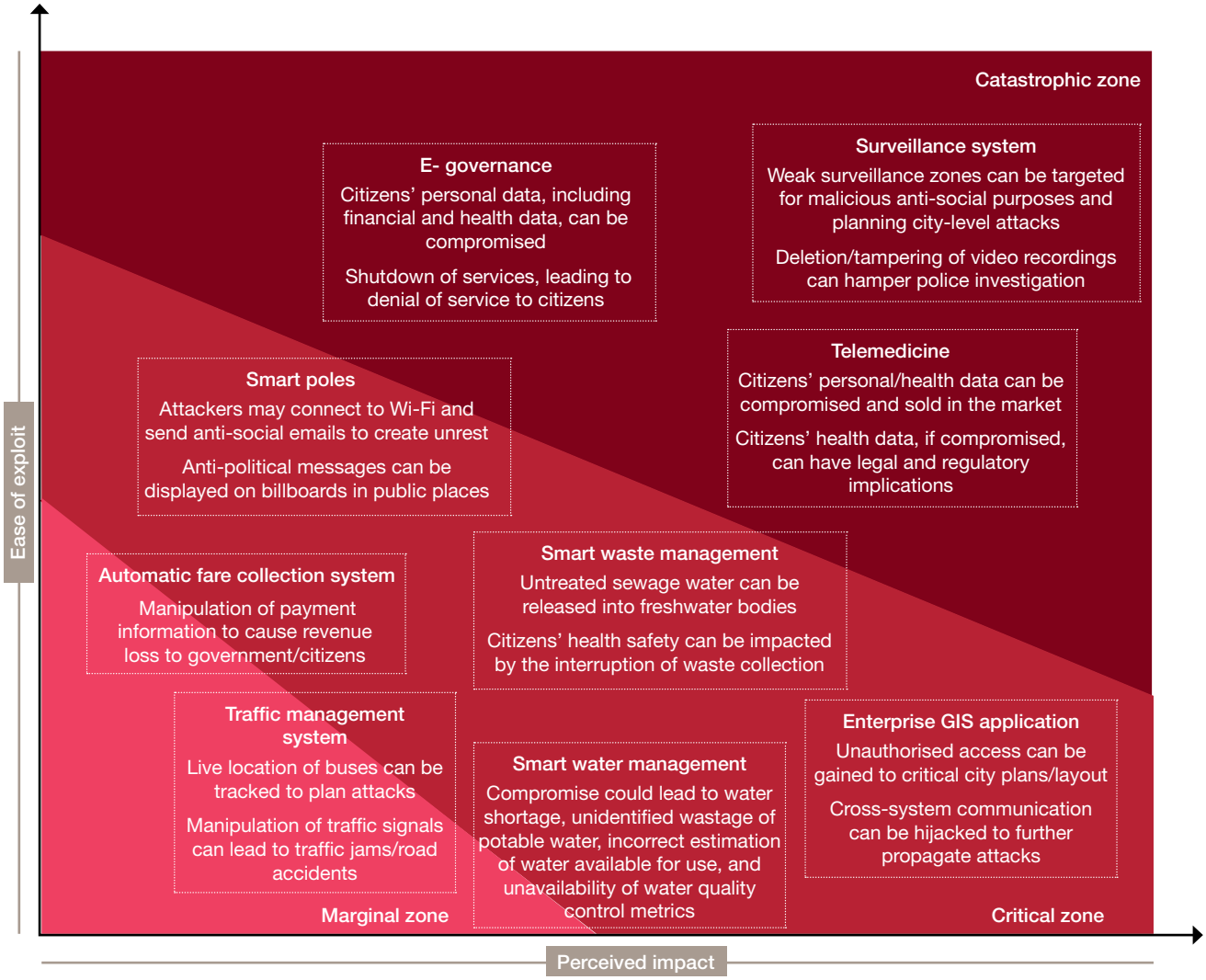
| Smart service | Vulnerabilities in systems associated with smart service | Potential risks |
|---|---|---|
| **E-governance** | • Unencrypted storage and transmission of citizen data<br>• Lack of user access and authorisation controls<br>• Multiple vulnerabilities due to non-adherence to software development life cycle (SDLC) process<br>• Outdated version prone to emerging attacks including ransomware | • Citizen personal data, including financial and health data, can be compromised<br>• E-governance services can be shut down, denying services to citizens |
| **City surveillance** | • Default password and configuration<br>• CCTV cameras accessible over open Internet with weak access controls<br>• Insecure transmission of video feeds | • Video surveillance can give information about weak surveillance zones which can be used for malicious anti-social purposes and to plan and plot a city-level attack<br>• Video recordings can be tampered/deleted, hampering police investigation |
| **Smart waste management** | • Inappropriate cryptographic techniques for security of radio-frequency identification (RFID) tags<br>• Cloning and spoofing of tags<br>• Denial of service attacks on tags | • Smart sewage system can be breached to open/close smart valves and release untreated sewage water into bodies of freshwater<br>• A denial of service attack can be performed to interrupt waste collection, posing a risk to citizen health safety |
| **Smart poles** | • Default password and configuration of smart pole edge devices (e.g. Wi-Fi, sensors)<br>• Inappropriate validation mechanism for connecting to edge devices (e.g. Wi-Fi)<br>• Remote terminal access to sensors | • Attackers may connect to Wi-Fi and send anti-social emails to create unrest in the city<br>• Anti-political message can be displayed in public places through digital billboards to stir unrest amongst the public<br>• Lights can be put off at night so that a crime is not captured by surveillance cameras |
| **Smart water management** | • Tampering of data during storage/transmission<br>• Cloning and spoofing<br>• Denial of service attacks | • Wrong data related to water management can lead to water shortage, unidentified wastage of potable water, and unavailability of water quality control metrics |
| **Telemedicine** | • Insecure storage and transmission of citizen health record<br>• Lack of user access and authorisation controls<br>• Business logic flaws in doctor consultation and medicine ordering | • Citizens' personal/health-related information can be compromised and sold illegally<br>• Citizens' health information can be compromised with legal and regulatory implications |
| **Automatic fare collection system** | • Cloning, forgery and tampering of smart cards<br>• Insecure transmission of financial data | • Payment information can be manipulated to cause revenue loss to government/citizens |
| **Enterprise GIS application** | • Unpatched vulnerabilities in GIS applications/application program interfaces (APIs)<br>• Insecure cross-system communication | • Unauthorised access can be gained to critical city plans/ layout<br>• Cross-system communication can be hijacked to further propagate attacks |
| **Intelligent traffic management system** | • Man-in-the-middle attack between sensor and reader<br>• Cloning and spoofing<br>• Denial of service attacks | • Miscreants can monitor the live location of buses and other parameters to plan an attack<br>• Traffic signals can be manipulated to create a traffic jam in the city |

## Categorisation of smart services based on risks

Considering the risks applicable to different smart city services, they can be divided into three categories based on the ease of exploiting the associated vulnerabilities and the impact level:

1. **Catastrophic zone:** The services categorised as catastrophic, if compromised, will impact safety and security, health, trust in the government, and privacy of citizens.
2. **Critical zone:** The services categorised as critical, when compromised, will pose a challenge to delivery only. However, these services may be further exploited to extend the damage and enter the catastrophic zone.
3. **Marginal zone:** If the services in this zone are compromised, citizens will be inconvenienced.

**Our analysis of the overall risks and vulnerabilities landscape for smart city services indicates that e-governance, CCTV surveillance and telemedicine are the most critical services for the Indian smart city.**




*It is important to note that smart cities are exposed to security risks that are capable of causing significant damage. Smart city stakeholders, both at the central as well as the smart city level, are required to take definitive steps towards securing the cities.*

# *Actions required by smart city stakeholders to enhance security maturity*

## A. Understanding the smart city stakeholders

At the central level, MoHUA is the key stakeholder, while at the smart city level, stakeholders include smart city special purpose vehicle (SPV), project management consultant (PMC), master system integrator (MSI), original equipment manufacturer (OEM) and third-party vendors.

### MoHUA

MoHUA is the apex body that sets up and monitors the Smart Cities Mission in India. MoHUA facilitates the formulation and administration of the rules, regulations and laws relating to housing and urban development.

**Smart city SPV**

The smart city SPV is accountable for the implementation and operations of a specific smart city with the objective of improving sustainability and livability. It drives the concept and execution of the smart city project, and helps build and activate teams to deliver smart services to citizens.

**PMC**

The PMC acts as an advisor/ consultant to the smart city SPV in achieving the vision for the smart city. The PMC manages the design, implementation and operations of the smart city, and ensures that quality smart services are delivered to citizens in a timely manner as per the procedures laid down.

**MSI/ vendors/OEM**

The MSI, along with the OEM, ensures that all smart services, solution systems and components are implemented and operated as per the requirements of the smart city. OEMs and other third parties provide an array of products and services for the efficient functioning of smart city services.

## B. Call to action

In order to secure smart cities, a collaborative effort is required from all the key stakeholders. Each stakeholder has to take the responsibility and play a definite role in securing the smart city.

**At the central level – MoHUA**

### MoHUA

- Develop detailed guidelines for implementing cyber security in smart cities. Though MoHUA has released the model cyber security framework for smart cities, there is an immediate need to provide detailed guidelines, including reference security architecture to smart cities for cyber security implementation.
- Mandate smart city SPVs to appoint security organisations with clearly defined security roles and responsibilities.
- Enforce the implementation of cyber security guidelines and link budget sanctions to the compliance status.
- Develop a cyber security enforcement mechanism to which subsequent budgetary sanctions must be linked.
- Encourage smart city SPVs to perform risk assessment and implement solutions leveraging custom-off-the-shelf (COTS)/Make in India/open source security products based on risk assessment, security budget, and MoHUA guidelines.
- Define security guidelines for the OEMs supplying products to smart cities.
- Create a platform for cyber security information sharing and knowledge transfer amongst the smart cities and other agencies (e.g. CERT-In, NCIIPC). Consider the set-up of smart city sectoral CERTs similar to the concept of other sectoral CERTs (e.g. financial CERTs, power CERTs) to ensure security across smart cities.

**At the smart city level**


The actions to be taken at the smart city level depend on the phase of development of the respective smart city in achieving its objectives. Smart cities can be at the following phases of development:

- **Planning phase –** from smart city nomination until on-boarding of MSI for implementation
- **Design/implementation phase** – from MSI on-boarding until implementation of smart city services
- **Operations phase –** post implementation of smart city services

There are definite actions that need to be taken for securing smart cities at various phases. The smart city SPV should ensure that these actions are executed by the respective stakeholders in a time-bound manner.

### Call to action – planning phase

**Smart city SPV**

- Appoint a chief information security officer (CISO) with defined security roles, responsibilities and accountability.
- Consider cyber security requirements in PMC RFP and PMC bid evaluation.
- Allocate budget for cyber security and privacy as part of the detailed project report (DPR).
- Ensure cyber security requirements are considered in MSI RFP and MSI bid evaluation.
- Include cyber security as agenda item in status update meetings conducted for the smart city.
- Ensure that the PMC team is adequately staffed with cyber security experts to oversee security design, implementation and operations.

### Smart city PMCs

- Perform security and privacy risk assessment to identify risk profile for smart city services.
- Develop smart city security architecture leveraging COTS/ Make in India/open source security products based on risk assessment, security budget and MoHUA guidelines.
- Include detailed specifications for security products, services and manpower in MSI RFP.
- Design robust security SLAs to measure and enhance security maturity on a continual basis.
- Review security architecture, solution, and implementation plan proposed by MSI from security and privacy perspective.

### Smart city MSI

- Propose a robust security solution in line with RFP requirements, MoHUA guidelines and applicable regulations.
- Ensure appropriate number of security experts with relevant skills are proposed as part of staffing.

## Call to action – design/implementation phase

### Smart city SPV

- Conduct monthly status update meetings to assess the quality of security implementation.
- Maintain contact with various security agencies such as CERT-In, NCIIPC and other security experts for cyberthreat advisory and incident reporting.
- Ensure that personnel with access to critical systems and information sign a non-disclosure agreement and go through a security clearance process.

### Smart city PMCs

- Review security and privacy policies and procedures prepared by MSI in line with international security standards such as ISO 27001 and NIST cyber security framework.
- Assess minimum security baseline guidelines for systems and devices, including operating system, databases, network and security devices, sensors, and IoT devices.
- Evaluate network security architecture and ensure security is considered across all four layers: sensor layer, communication layer, data layer, and application layer in line with MoHUA guidelines and NIST IT reference architecture.
- Review the high-level and low-level designs (HLD and LLD) for solutions and applications from the security and privacy perspective.
- Review compliance with security architecture, policy, procedures and minimum baseline security guidelines during implementation status update meetings.
- Review business continuity and disaster recovery plans prepared by MSI.
- Ensure security assessment is conducted and identified vulnerabilities closed before user acceptance testing (UAT) sign-off and Go-live for each solution.
- Prepare and disseminate cyber security related awareness material for different stakeholders, including smart city SPV, MSI, third parties, and citizens through appropriate mode.

### Smart city MSI

- Prepare and obtain sign-off for all design documents, including but not limited to:
  - Security and privacy policies and procedures
  - Minimum baseline security guidelines
  - Security architecture
  - Business continuity and disaster recovery plans
  - Application and solution HLD and LLD
  - SLA management framework

- Implement security across the four layers as per security policies, procedures and minimum baseline security guidelines:
  - Sensor layer
    - Authenticate edge devices, including IoT and environmental sensors, while installing the network based on physical characteristics such as device ID and MAC ID.
    - Disable physical interface in edge devices to prevent software modifications.
    - Enforce authentication for remote access to all edge devices.
    - Change default passwords of all edge devices.
    - Harden all edge devices in line with the minimum baseline security guidelines.
    - Encrypt all communications to and from edge devices.
    - Configure edge devices to connect to authorised wireless network only.
    - Regularly update edge device firmware to prevent known attacks.
    - Secure over-the-air updates to edge devices via encrypted channel.
  - Communication layer
    - Segment data centre network into multiple zones such as demilitarised zone, trusted zone, management zone, production zone and user zone.
    - Place all edge devices, including Wi-Fi, sensors and IoT devices, on a separate firewall-monitored network.
    - Secure the data centre network through external firewall, web application firewall, and intrusion prevention and detection system, and other security products.
    - Configure wireless network, wherever required, securely in line with guidelines published by the Department of Telecom.
    - Implement authentication and hardening for all the devices on the network.
    - Encrypt inter-component communication with secure protocols such as HTTPS over TLS 1.2, SSH, SFTP, etc.
    - Use encrypted channels such as virtual private network while connecting remotely to the data centre network.
    - Disable unused network or telecommunication access points to prevent unauthorised access.
  - Data layer
    - Implement user authentication on databases.
    - Provide database access to authorised users only on a need-to-know basis.
    - Deploy the database server into a segmented zone, separate from the app server and web server.
    - Perform hardening for all database servers as per minimum security baseline guidelines.
    - Perform channel encryption to ensure security of data in transit.
    - Encrypt all sensitive data and store encryption keys in a trusted key store.
    - Conduct regular backups of database and encrypt backup media.
  - Application layer
    - Follow secure SDLC process for custom developed applications.
    - Provide privileged access to servers to authorised users only.
    - Perform hardening for all application servers and web servers as per minimum security baseline guidelines.
    - Build authentication mechanisms for all applications and API.
    - Create a role-based access control list derived from the principle of least privilege.
    - Secure application communication through encrypted protocols such as HTTPS over TLS 1.2 and above.
    - Validate user-provided inputs at server side.
    - Implement error-handling mechanism on end-user inputs.
    - Disable access to default web server pages.
- Implement cloud security solution in line with Guidelines for Government Departments on Contractual Terms Related to Cloud Services released by the Ministry of Electronics and Information Technology (MeiTY).
- Provide privilege access to systems, applications, network and sensors to authorised users only on a need-to-know basis.
- Design and implement a SOC with advanced analytical capabilities to detect, respond, and recover from security incidents on a 24*7 basis.
- Ensure integration of all systems and devices with the SOC.
- Perform security testing of all applications and devices, and close identified gaps before service go live.

## Call to action – operations phase

### Smart city SPV

- Conduct frequent cyber security review meetings with PMC and MSI to address security issues and enhance security maturity.
- Ensure security and privacy policies are reviewed annually.
- Report security incidents, if any, to CERT-In and NCIIPC on a timely basis.
- Ensure periodic submission of MoHUA guidelines compliance report by MSI.
- Appoint an independent security audit agency to regularly assess the security posture of the smart city.

### Smart city PMCs

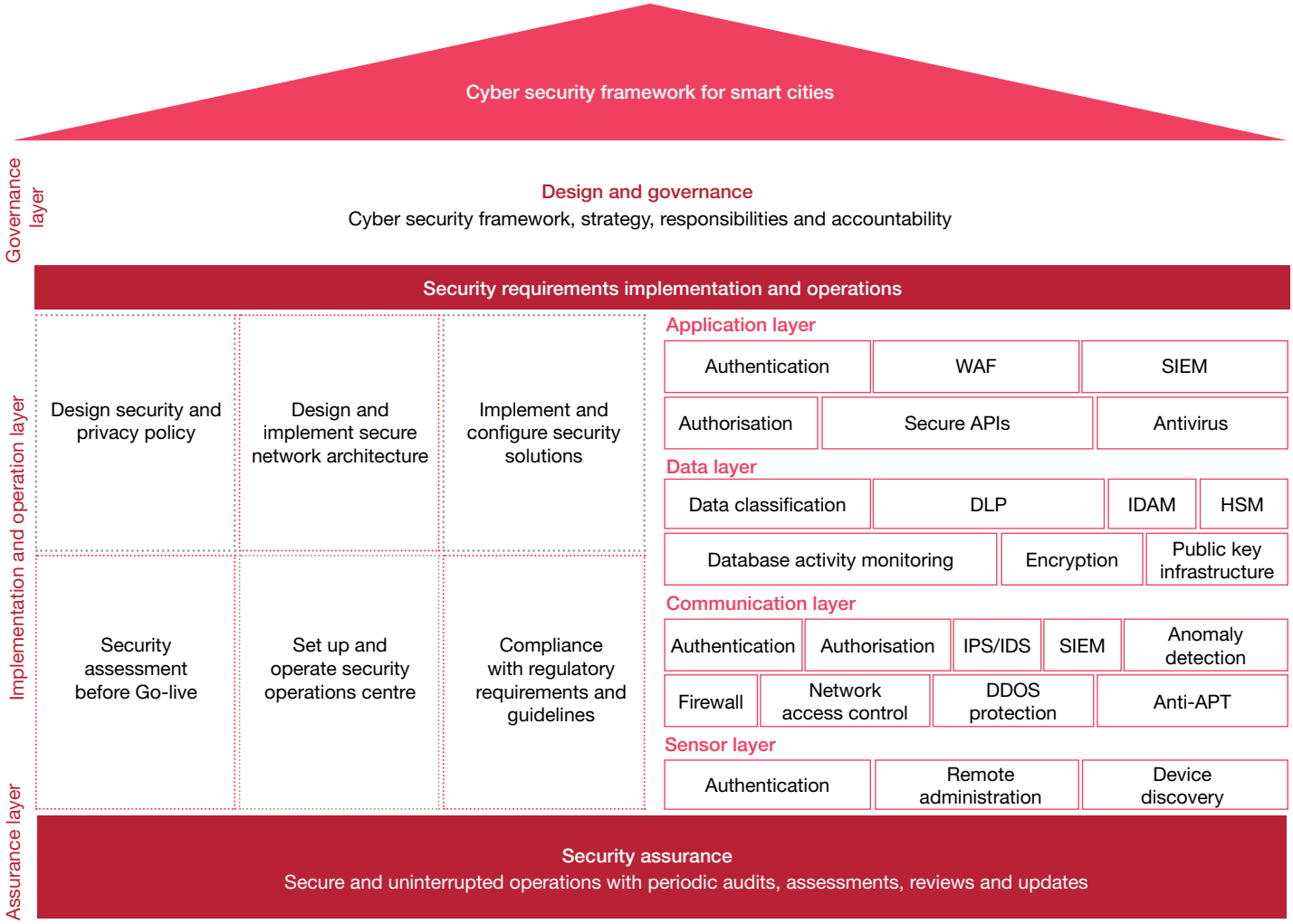
- Periodically review the smart city's security and privacy policies, procedures, and minimum baseline security guidelines to keep abreast of emerging risks.
- Ensure periodic security assessments of all applications, websites, network and edge devices are conducted by MSI.
- Periodically review security-related SLAs and identify trends and areas of improvement.
- Conduct periodic security training and awareness sessions for different stakeholders.
- Perform gap assessment to assess compliance with MoHUA guidelines.
- Regularly review the security posture, and present risk dashboard to smart city management on existing and emerging cyber risks, trends and directives.

### Smart city MSI

- Create an asset inventory and identify critical systems and devices ('crown jewels').
- Update all the systems/devices with the latest patches on a regular basis.
- Follow secure operational procedures, such as user access management, change management, incident management and capacity management, during smart city operations.
- Operate the SOC on a 24*7 basis.
- Periodically review firewall rules and appropriately set firewall rule base to allow for only authorised incoming and outgoing traffic.
- Report and respond to security incidents, if any.
- Perform periodic user access reconciliation for systems, applications and devices, and revoke unauthorised accesses, if any.
- Perform periodic testing of business continuity and disaster recovery plans.
- Perform periodic backup of information, software and systems in accordance with backup policy.
- Track and close observations identified during assessments performed by different agencies, including PMC, independent audit agency, and any other agency.
- Follow secure SDLC process for any enhancement to smart city applications and solutions.

# *Cyber security framework for smart cities*

While the action points will help the smart city SPVs to make the cities secure, embracing a robust cyber security framework will give holistic coverage of security. A cyber security framework for smart cities has been designed using MoHUA's Smart City Cyber Security Guidelines. It covers multiple aspects—security governance, implementation, and operation of security products and services, and security assurance. The framework ably secures all the layers of technology, allows each smart city to align its requirements and helps comply with the changing regulatory landscape.




**The various layers of the framework have been detailed out below:**

## Design and governance

- Appoint a security organisation led by CISO to ensure cyber security in the smart city.
- Perform a business-driven risk assessment to appropriately consider cyber security requirements.
- Design a security and privacy framework including policy, procedures and minimum baseline security guidelines covering systems, network devices, and edge devices including IoT, sensors, etc.
- Establish a governance mechanism to periodically review and enhance cyber security for the smart city.
- Plan for cyber security awareness and capacity building within the smart city.
- Maintain contact with various security agencies such as CERT-In and NCIIPC and other security experts for cyberthreat advisory and incident reporting.


### Security implementation

- Design and implement smart city security architecture leveraging COTS/Make in India/open source security products based on risk assessment, security budget, and MoHUA guidelines.
- Implement the security products across different layers: sensor layer, communication layer, data layer and application layer.
- Ensure that all the systems, network and edge devices are configured as per the minimum baseline security guidelines.
- Perform security assessment of the services and close identified gaps before Go-live.

### Security operations

- Conduct security operations in line with the security procedures—change management, incident management, etc.
- Design, implement and operate a security operations centre (SOC) with advanced analytical capabilities and integrate with all the systems and edge devices, wherever possible. Operate the SOC on a 24x7 basis to detect, identify and respond to security incidents.
- Enforce a comprehensive patch management process including regular and timely updates of all firmware and operating systems.
- Periodically test business continuity and disaster recovery plans for smart services.

### Security assurance

- Set up an assurance process to regularly review the security posture, and enhance cyber security maturity.
- Perform regular vulnerability scanning of firmware, operating system, applications, API, etc., to identify and mitigate existing security vulnerabilities. Perform regular configuration reviews of all systems, network and edge devices to ensure security is continuously maintained.
- Review the security-related SLAs on a regular basis and identify areas of improvement.
- Conduct periodic reviews against regulatory requirements and enhance overall security maturity.

# Notes

# Notes

# About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. www.dsci.in

# Contacts


**DSCI team**

**Amit Verma**
Deputy Director, DSCI
Email: amit.verma@dsci.in

**Manishree Bhattacharya**
Manager – Research, DSCI
Email: manishree@dsci.in

**Industry development team**
Email: industry@dsci.in


# About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 2,36,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.



# About the authors

This report has been co-authored by Sivarama Krishnan, Rahul Aggarwal, Anas Viquar, Vikas Sood, Suman Bhunia, Amit Verma, and Manishree Bhattacharya.

Sivarama Krishnan leads the Cyber Security practice at PwC India. Rahul Aggarwal is a Partner and focuses on cyber security within the government practice. Anas Viquar and Vikas Sood are Associate Directors in Cyber Security and focus on smart cities. Suman Bhunia is a Manager in Cyber Security and focuses on IoT security.

Amit Verma and Manishree Bhattacharya are part of Data Security Council of India (DSCI) and focus on industry development and research in cyber security and data privacy.

# Contact us

**Sivarama Krishnan**
Leader, Cyber Security
sivarama.krishnan@pwc.com

**Siddharth Vishwanath**
Partner and Cyber Advisory Leader
siddharth.vishwanath@pwc.com

**Rahul Aggarwal**
Partner, Cyber Security
rahul2.aggarwal@pwc.com

**Neel Ratan**
Leader, India Government Sector
neel.ratan@pwc.com

**Rakesh Kaul**
Leader, Government and Public Sector
rakesh.kaul@pwc.com

**NSN Murty**
Leader, Smart Cities
nsn.murty@pwc.com

pwc.in



SG/September2018-14660