Cyber Risk Mitigation for Smart Cities

Abstract

Rapid growth in global population and evolving technological, macro-economic, and environmental landscapes have fueled widespread interest in smart cities, which are, essentially, dynamic ecosystems characterized by highly advanced, intuitive, and interdependent cyber systems. As emerging digital technologies and the Internet of Things

(IoT) pave the way for these smart habitats, effective risk management becomes crucial to provide risk-free smart services to citizens.

Approximately 70% of the world's population is expected to live in cities by 2050.

Two key features of smart cities are citizen-centricity and digitally-enabled infrastructure.

The Rise of Smart Cities

As with all IT-enabled services, smart city services too should be risk-free and secure. In connecting devices and users, cyber systems should ensure the highest level of confidentiality and integrity, while allowing unhindered availability. It is therefore important to proactively manage the security risks of interdependent systems of the smart city digital infrastructure.

Apart from smart infrastructure, a smart city has advanced systems to manage energy, transport, traffic, water, healthcare, and education. It is a seamless union of technology, government, and society to enable smart living, which is characterized by a booming economy, effective governance, and convenient public services.

Interdependent Systems Form the Backbone of Smart Cities

Interdependent systems are the foundation of smart cities, as they provide the critical infrastructure to handle major public systems and citizen services. These include water and energy generation and transmission setups, transportation frameworks, waste disposal mechanisms, street and home lighting systems, connected healthcare, surveillance, and more. Interdependent systems also enable dynamic and synergistic data gathering and analytics, which drive continuous improvements across systems. In effect, a smart city is a 'system of systems' that follows a scale-free topology to allow future expansion, but without affecting the attributes of interdependency and interconnectedness..

- **Opportunities and Risks:** IT-enabled interdependent systems present several opportunities to improve a citizen’s lifestyle. They can help city councils take necessary actions, based on real-time analysis of the data collected from various interdependent systems, such as identifying health hazards, mapping energy efficiency of buildings, preventing crime, and effectively managing natural disasters. However, these interdependent systems also pose operational challenges and security risks. If one smart service information system fails to provide relevant information to other connected smart services, it can lead to chaotic situations.

- **Criticality of Risk Mitigation:** Due to the large number of connected devices that make up a smart city's digital infrastructure, enhanced security management for gateway devices, such as industrial control systems (ICS) and IT systems (ITS), is critical to prevent data breach or leakage. Leakage of sensitive data can lead to a lockdown of critical services.

The Role of Smart City Councils

Risk mitigation in smart cities requires a detailed understanding of several factors. These include design and architecture of smart services, IT infrastructure support capabilities, and the knowledge of probable cyber threats. A city council should operate like a modern-day enterprise with specific goals and objectives that include planning for defending against cyber-attacks and responding to emergencies.

- **Ensuring security of network and sensors:** The smart city council should secure connected systems and sensors from any physical attack or infiltration. Identity management and device authentication mechanisms should be deployed at every interface of a smart system. Digital forensic capabilities, which help trace cyber breaches and gather evidence of malicious activities for legal action, should be integrated with the overall cyber architecture, right from the design phase. Gathering and analyzing real-time data with supervisory control and data acquisition (SCADA) will help predict security failures, and thus prevent a complete lock-down of critical services.

- **Building resilient systems:** As a smart city grows, the interconnections of systems and interdependencies of smart services increase manifold. This makes them more vulnerable to cyber-attacks. The smart city council should therefore aim to design risk resilient digital architecture. The architecture should possess the adaptive capability to arrest anomalies in the nascent stage, and lock down a subsystem without disturbing other live components, ensuring uninterrupted service delivery.

- **Adopting international standards:** The security standards and risk mitigation strategies currently being used to secure IT systems may not be adequate to safeguard the interdependent systems in smart cities. ISO 22301:2012, the International Standard for Societal Security — Business Continuity Management Systems[1] should be adopted to prevent the disruption of citizen services. Proper communication management is critical for smart cities to respond to cyber threats and other exigencies.

- **Performing system impact and interdependency analysis:** Periodic system impact analysis should be performed to identify risks posed to critical interdependent systems and interconnected services, with appropriately defined recovery time and recovery point objectives. Smart cities should also have secure data receivers and data storage to collect and store data generated from the ICS and ITS components for analysis, decision making, and incident response management. Smart city councils should devise a component protection strategy to identify critical components of interdependent systems for agile risk analysis.

The CPNI Good Practice Guide for Process Control and SCADA Security-[2] can be used by city councils to ensure security and trustworthiness of the interdependent systems. It provides a framework based on industry best practices for process control and IT security. The framework focuses on seven key themes:

1. Understanding business risks
2. Implementing secure architecture
3. Establishing response capabilities
4. Improving awareness and skills
5. Managing third party risks
6. Engaging projects for security measures in service design
7. Establishing ongoing governance

- **Ensuring citizen compliance:** Citizens of smart cities are bound to play a crucial role in ensuring the security of interdependent systems from cyber as well as physical security perspectives. Citizens with smart devices are critical points in the cyber system framework, and can be targeted by attackers and hackers to gain entry into the system. This can be done through social engineering, spam emails, data streaming, and other malicious methods. To prevent this, smart city councils should develop policies and procedures for establishment, maintenance, and operation of secure smart services. Cyber-awareness programs should be made mandatory for citizens, and penalties levied for non-compliance.

Conclusion

Understanding and evaluating risks in smart city systems require a pragmatic approach to cyber risk management due to the high level of interconnectedness of smart services and the rapidly evolving nature of constituent systems. With smart cities projected to grow rapidly over the next few years, there is a clear need for smart city councils to focus on mitigating security concerns. Incorporating risk mitigation and developing strong security strategies in the initial planning and service design stages will enable smart city councils to provide safe, secure, and reliable services to its citizens.

References

[1] ISO, 2012. ISO 22301:2012, http://www.iso.org/iso/catalogue_detail?csnumber=50038, accessed November 2015

[2] Good Practice Guide – Process Control and SCADA Security, http://www.cpni.gov.uk/Documents/Publications/2008/2008031-GPG_SCADA_Security_Good_Practice.pdf, accessed November 2015

About The Author

Abhik Chaudhuri

Abhik Chaudhuri is a Domain Consultant with the Information Technology Infrastructure Services Global Technology Practice at TCS. He is a Chevening TCS Fellow in Cyber Security, Privacy and Policy with more than 14 years of IT experience.

Contact

Visit TCS' IT Infrastructure Services unit page for more information

Email: itis.presales@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty.

IT Services
Business Solutions
Consulting

TCS Design Services I M I 12 I 16