SECURING
SMART
CITIES

The Smart City Department Cyber Security role and implications

Authors:

Mohamad Amin Hasbini, *Senior Security Researcher, Kaspersky Lab*

Cesar Cerrudo, *CTO, IOActive Labs*

David Jordan, *CISO, Arlington County Government, Virginia, USA*

Ramzi El-Haddadeh, *Associate professor, Management Information Systems, Qatar University*

Alan Seow, *Cyber Security Practitioner*

Samir Pawaskar, *Cyber Security Policy and Standards Section Head, Qatar Ministry of Information and Communications Technology Team*

SECURING
SMART
CITIES

CONTENTS

SECURING SMART CITIES

Ver. 1.1: picture on page 6 has been replaced; a typo on page 11 has been fixed.

Ver. 1.2: Removed expired reference on page 10

1 INTRODUCTION

Interest in the smart city concept has grown exponentially over the past few years, with top research being done in the Internet of Things (IoT) and urban domains to define, assess, and improve smart city services and offerings. In smart cities, information security plays a major role in protecting the higher levels of confidentiality, availability, and integrity as well as the stability that national services and organizations need to support sustainable and livable smart environments.

Smart city stakeholders are identified as the government, the commercial organizations and the citizens; the development of a smart city organization or business has also been identified to heavily rely on technology and service providers (1); but as each organization requires its own smartness assessment and development, it has become clear that responsibilities, processes execution and decision making need to be institutionalized, where “smart city departments” or “smart city offices” get established to take ownership of the arrangement to become “smart city compatible” and to prepare roadmaps for the future of the organization itself; much like the IT departments in the 2000s, independent smart city departments are expected to emerge in organizations isolating organisation’s political aspects from the technological aspects (8)(1).

According to the Institute for Electrical and Electronics Engineers (IEEE), “*a smart city brings together technology, government and society to enable the following characteristics: a smart economy, smart mobility, a smart environment, smart people, smart living and smart governance.*” This can be realized using a wide range of connected systems to process and exchange data between multiple stakeholders, including transportation, energy, and city services. As new points of connection are introduced throughout a city, having processes to methodically evaluate the security risks and appropriate mitigations for each connected system inside each organization is critical to the overall success of the city, the smart city is an ecosystem of smart organizations, where tolerance to cyber damage is little compared to the current world, more comparable to critical infrastructure environments, but much more demanding. Smart City Departments (SCD) are expected to emerge in smart city organizations (Governments and Businesses) to manage the city requirements and control its operations.

In previous document on the Cyber Security Guidelines for Smart City Technology Adoption, we identified the cyber security planning, evaluation and operational requirements for smart city technologies; this document discusses the Smart City Department information security

role, its influence on technology adoption, services quality, legislative compliance, interorganizational and intraorganizational information and communication resilience in addition to the efficiency and sustainability of operations. The purpose is to provide guidelines for public and private organizations when planning and building their SCDs, that could be used as a baseline for the role development of emerging smart city departments or similar functions, helping provide a certain level of assurance and trust to operations and services, thus supporting the promotion and propagation of smart city services. It describes the types of roles and responsibilities to be defined and adapted for a successful consideration of information security issues in smart environments, risk control and organizational readiness for cyber occurrences. This guide is not a detailed testing or assessment program, but rather an illustration of the key elements that organizations need to examine and be aware of, when defining the role of smart city departments, in order to achieve the best safety and resilience.

2 THE SMART CITY DEPARTMENT

In reality, SCDs or similar functions, have already been established in a number of cities and large organizations to initialize planning and long term preparation for the transformation, development and compatibility of organizational business for smart city requirements.

SCDs or similar functions are expected to be present in most smart city organizations. Initially helping in adapting efforts and changes needed to transform business processes and practices to better support smart environments, but also directly governing organizational performance, smart city compliance, legislative communication and collaboration with the smart city government entities.

SCD teams have the responsibility to command smart city transformation and recommendations to adapt and guide the operations towards a smart eco-system. SCDs could have large scale roles (city level) or scoped scale roles (organization level). SCDs role could be defined as the following:

- SCDs are expected to collaborate with leadership to define the business model, organizational roadmap, services catalog and roll out plans, in addition to creating a revenue model to provide assurance for the business sustainability.

- SCDs will be the main interface for smart city operations, leading communication with other smart city organizations or government entities; SCDs need to ensure compatibility and full harmony with the smart city complex correlation engines or what are also called the “systems of systems” (ISO/IEC 15528 Systems Engineering – Systems Engineering Life-Cycle). (2)(3)(4)

- SCDs will be in charge of stakeholders communication, strategy agreements, setting roles and responsibilities, process execution and control.

- SCDs will also require visibility over operations, functions, processes and their status, measuring performance, security and quality.

- SCDs will then be required to evaluate business resilience, measure organizational smartness and transformation progression.

While the introduction of the SCD in smart city organizations can help in maintaining the anticipated technological and organizational alignment, the functionalities and contributions within this department will need to be more than just a typical cost reduction and productivity enhancement activities. In this respect, smart city organizations will need to ensure that there is somewhat a realization of the technological and business values reflected on its re-defined business models. In particular, this will help smart city organizations in leveraging their success improving return on investment (ROI), and maintaining competitive advantage in smart environments.

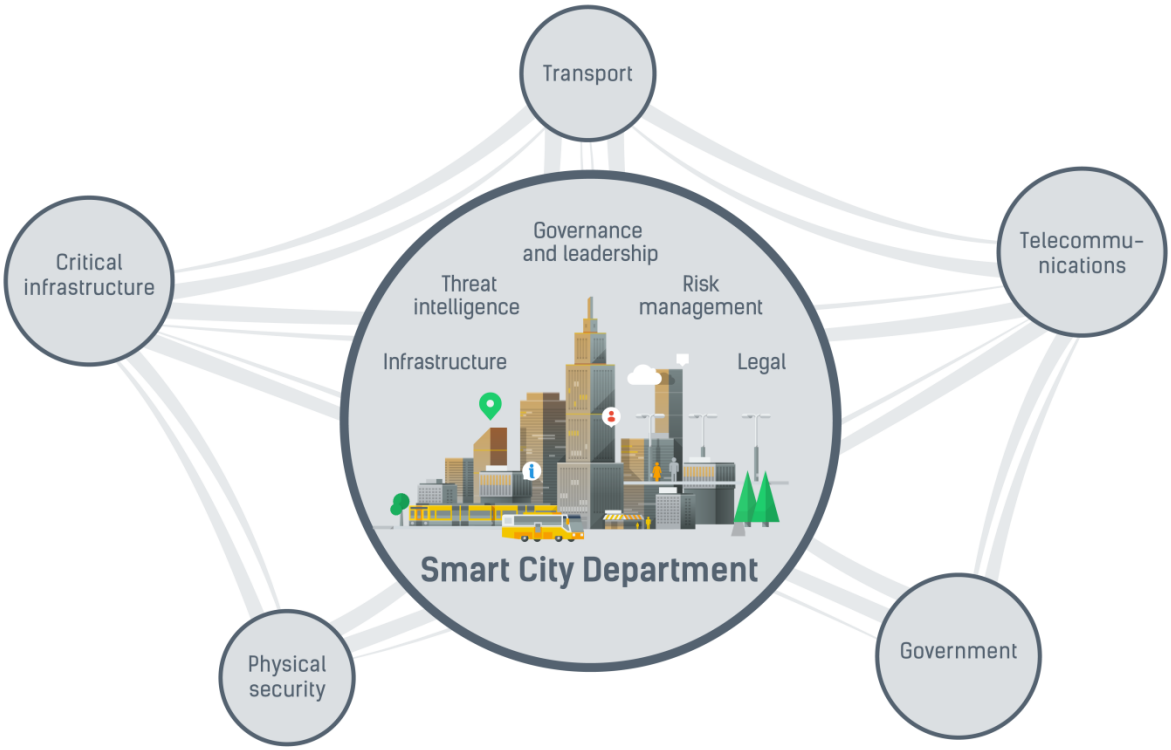
3 THE SCD CYBER SECURITY RESPONSIBILITIES

Previous research(6)(5)(7) has already identified the biggest security challenges for the smart city environments, which can be summarized as the following:

- L**arge and Complex attack surface:** The smarter the cities, the more systems and “systems of systems” they will incorporate, increasing the risk and impact of an attack, thus requiring better control and visibility. Furthermore, what adds to the smart city systems complexity is the integration between vendor’s solutions, especially during fast evolving technological transformations.

- **Insufficient oversight and organization:** Complex systems will then require stronger management and governance capabilities; in addition, keeping leadership fully knowledgeable of complex occurrences requires more resources and capabilities.

- **Direct political impact:** Complex environments need to be directly managed by the political leadership. Hence, an identified political appointee of government cabinet function overseeing SCD coordinating effort is desirable as changes in decision making priorities has a direct impact to systems development, budgets and resources.



In the following we identify the major cyber security related roles that could be played by the smart city departments in order to maintain a safe environment, starting from the period when the organization is migrating towards the smart city or in later stages of its maturity.

3.1 GOVERNANCE AND LEADERSHIP SUPPORT

SCDs are responsible for digesting cyber security organizational requirements, supporting the Information security team in defining the technologies needed and the cyber security strategy to be adopted; such also need to be communicated and made fully understandable to decision makers, helping them make the right decisions around investments and business/organizational functions.

The role of the SCD in defining the cyber security requirements for smart operations is essential for the following reasons:

- They are in communication with the different stakeholders, always up-to-date with the business goals and risks.

- They are aware of the compliance requirements for the cyber security obligations and regulations provided by the government.
- They are responsible and aware of the technical and business operations that are being effected in the smart city, therefore capable of influencing these with policies and controls, to maintain safety and resilience.

Having visibility and guidance capabilities enables the SCDs to directly Influence top management support for projects as per the inferred priorities, SCDs should be at the core of the organization, with technological and business competences, which accordingly should be reflected on the department human capital.

3.2 INFRASTRUCTURE SUPPORT

The SCDs have a role of defining organizational strategy in the smart city, based on the organizational goals, therefore putting them in direct influence over technologies adoption; they will also need to assess performance contrasted onto business goals and compliance requirements. Having direct communication with the different stakeholders, the SCDs could be required to monitor cross-organizational related occurrences including cyber threats, requiring conformity from the partners and stakeholders to the protection of operations.

SCDs visibility over the operations and data location, enables them to support the definition of critical data locations but also the levels of protection needed to maintain the safety of clients and regulatory compliance (data classification and related security controls/policy). SCDs communication with other external entities would also give them better visibility over competitive operations and might help them adapt or recommend practices to strengthen processes and functions. In addition, SCDs are expected to establish communication with vendors and solution developers, to designate agreements on the minimum security baseline and emphasize only highly secured and thoroughly tested products are rolled out. It is also important to designate a governmental role in this case, to regulate publicly accessible solutions by vendors and businesses, verifying adequate compliance and control over offered smart city services.

3.3 RISK MANAGEMENT OPTIMIZATION

The input from the SCDs to the risk management teams is highly important to guarantee the full awareness of the parties on risks and threats in addition to sudden fluctuations that could happen (new risks, vulnerabilities, threats, etc.); Having such input, the risk department is required to investigate priorities and conclude with the relevant recommendations for the business.

Liability on the other side needs to be very well defined and measureable, ownership of missions and systems is important for fully defined roles and responsibilities. Being well defined, liability measures and policies need to be approved by management and legal departments, but also communicated to all employees, partners and clients. In a connected world, damage could be easily done, then and only then that strictly defined liability measures will be tested for efficiency.

3.4 LEGAL SUPPORT

The legal aspects of the smart city organizations need to be well defined in contrast to government regulations and partners. Roles, responsibilities and mission ownership are also expected to be fully defined to facilitate lawful operation of the business.

Ensuring services quality is crucial for the survival of the organizations in smart environments, SCDs should be actively coordinating inter-departmental collaboration activities to ensure the most efficient operations avoiding redundancy, but also provided permission to require prioritized tasks from other organizational departments. SCDs are also expected to balance and negotiate the service quality with providers and customers as per the organizational goals, in synergy with the legal department(s).

3.5 COLLABORATIVE THREAT INTELLIGENCE

Threat intelligence is already a main source of defense for many organizations. Knowledge about worldwide and regional cyber activities is key to the identification of possible attacks on an organization. SCDs will require the establishment of threat intelligence capabilities in complex environments. Collaborative threat intelligence capabilities are key to the detection of even the smallest attacks. Organizations are expected to proactively monitor events on networks within their visibility (including partners and 3rd party) to collect threat data that could be shared on a global or city scale threat intelligence systems, enabling the automated propagation of threat data and relevant protection to other parties.

The SCDs will have access to different sources of threat intelligence, whether from internal departments or from external sources such as clients, partners, government; they are also expected to have full coordination with the relevant government entities (such as Computer Emergency Response Teams) responsible for the collection, analysis and dissemination of threat data.

4 CONCLUSION

Smart cities are becoming a reality, many cities around the world are reinventing themselves into the digital world and more than 80 cities are expected to be smart by 2025. It is imperative that cities transform themselves in the most planned, efficient and speedy methods, building on existing human capital and infrastructure capabilities, delivering a certain level of assurance and trust to operations and services, thus promoting and propagating services; after all, the smart city is a place where the living experience is better through the eyes of the people. The smooth transformation of the city is key for the right adaptation of its stakeholders and the happiness of its citizens.

REFERENCES:

(1)
(2) http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63711
(3) http://www-935.ibm.com/services/us/gbs/bus/html/ibv-smarter-planet-system-of-systems.html
(4) http://www.juniperresearch.com/document-library/white-papers/smart-cities-system-of-systems
(5) http://www.darkreading.com/vulnerabilities---threats/smart-cities-4-biggest-security-challenges/d/d-id/1321121
(6) http://www.ioactive.com/labs/resources-white-papers.html
(7) http://securingsmartcities.org/wp-content/uploads/2015/11/Guidlines_for_Safe_Smart_Cities.pdf
(8) http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6525605

CONTRIBUTORS:

Krishnakumar Kottekkat

Ryan Naraine

Ivan Shadrin

Craig Brophy

Sandeep Singh