Transformational ‘smart cities’: cyber security and resilience

Towards the century of **smart cities**

Confidence in a connected world. Symantec

Contents

Introduction

For the first time in history, more than 50% of the world's population lives in cities.

This urban growth will bring benefits and challenges. Demographic and social ecosystems will need to evolve; economies will be under increased pressure; the environment will be challenged; city governance will have to adapt; digital and social inclusion needs will grow and healthcare and education provision will demand a new approach.

In order to address these challenges, cities need to become, and in many cases are already becoming, 'smart', by ensuring a more rational approach to the way services are operated and delivered, and aiming at a better and more sustainable quality of life for city dwellers. There are many definitions of 'smart city' and many criteria and characteristics to classify them.

Here we will refer to the fact that 'smart' delivery of services relies on Information and Communication Technology (ICT) as a key enabler and that the systems involved can profit from the ability to be highly interconnected through various technologies.

However, in order to guarantee service continuity and integrity, the ICT systems that oversee and control a 'smart city' need to be designed, from inception, with cyber security, robustness, reliability, privacy, information integrity, and crucially, resilience, in mind.

This report will explore the requirements and challenges of creating a secure, reliable and resilient smart city. It will consider how administrations and the overall city ecosystems will need to provide innovative, resilient 'smart' solutions that leverage digital information while protecting against malicious violations, unintentional damage and natural disasters.

Urban challenges

For the last few decades, visionary city administrations have started looking closely at ways to enhance quality of life for city dwellers. However, with today's constrained resources, they face new and wide-ranging pressures:

- Population growth places increasing demands on new and existing services, sometimes to the detriment of quality.
- The prolonged economic crisis has progressively eroded investments in services for citizens.
- Central government has to comply with international carbon emission targets and cities play a major role in emission production.
- As energy requirements grow, pollution increases, supply needs to be managed efficiently and critical infrastructure needs to be protected.
- Ageing urban infrastructure can be a ticking time bomb, especially in recessive economies.
- Public safety and security is becoming increasingly challenging.
- Citizens are becoming more demanding, particularly the younger population of so-called 'digital natives'.
- People are increasingly using unsecured Wi-Fi hotspots to access personal information (email, social network, Internet banking) and exposing themselves to various types of attacks.

City governments are expected to address all of these challenges, on top of existing issues. This drives the need to create an ecosystem of ICT vendors, energy suppliers, building companies, health providers and education bodies; all engaged in providing state-of-the-art solutions in every field.

City competition: drivers and stakeholders

A McKinsey Global Institute analysis suggests that just the top 600 cities (defined by their contribution to global GDP growth to 2025 – a group they call the City 600) will generate nearly 65% of world economic growth in this period[5].

Modern cities compete with each other to attract businesses, talent, skills and taxpayers. As a result, administrations are becoming entrepreneurial, valuing innovation, technology, marketing and communication.

In turn, businesses are attracted into cities by the ease of operation that they offer, in terms of cost efficiency, infrastructure (office space, broadband, telecommunications, as well as utilities such as energy, water and transportation), and general quality of life for staff (residential, healthcare and education systems).

The smart city ecosystem is a broad partnership between the public and private sector (PPP). City planners and developers, non-governmental organisations, IT system integrators, software vendors, energy and utility providers, the automotive industry, and facility control providers, as well as technology providers for mobile technology, cloud computing, networking, Machine-to-Machine (M2M) and Radio-Frequency Identification (RFID), all have a role to play.

An increasingly important role is also played by central governments: cities prosper, or decline, within the fabric of states, nations and regions so there is a need for integration within this economic and social framework. Smart cities are seen as a new opportunity for citizens and investors, so central government can play a formidable role in encouraging municipalities to adopt smart measures.

One of the most remarkable examples of central administrative involvement in the smart city discipline comes from the UK, where the government, through its Technology Strategy Board (TSB), has launched 'The Future Cities Demonstrator', an initiative that has awarded £24 million to the city of Glasgow for the best smart city project amongst UK municipalities.

The European Union is also actively promoting smart city initiatives, with funds for research and sustainability targets for member states.

Resilience and cyber resilience

1. ***Resilience:*** *The ability of an ecosystem to return to its original state after being disturbed (Collins Dictionary)[1].*

2. ***Resilience:*** *The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents (USA Department of Homeland Security)[2].*

3. ***Cyber resilience:*** *The organisation's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace (Information Security Forum)[3].*

4. ***Cyber resilience:*** *The ability of systems and organisations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery (World Economic Forum)[4].*

The integrated and interrelated smart city and its key functional areas

The smart city experience involves systems and objects interconnected through various technologies, like local, wide and wireless networks.

The "Internet of Things" (IoT) concepts apply here in terms of multitude of devices interacting with control units and dashboards, through sensors, RFID, M2M, satellite and GPS.

Gartner defines the IoT as *"the network of physical objects that contain embedded technology to communicate and sense or interact with their internal state or the external environment"*[6].

The amount of data generated by these systems can reach a considerable size. Big Data will need to be appropriately and centrally stored, managed, analysed, and protected.
The city operation's centre will supervise the interaction between systems and will have to ensure continuity, integrity and resilience.

With time, the interconnected and interdependent services of smart cities will evolve under a centralised governance dashboard of specialised stakeholders, responsible for setting policies and processes, managing ICT assets, services and protocols, and ultimately administering the services for constituents. ICT control and management capabilities will be crucial, to guarantee an efficient, secure and resilient governance and delivery.

The systems, disciplines and technologies involved, can include:

Smart grids and energy efficiency

It is estimated that cities are responsible for between 60% and 80% of the world's energy use. Optimising delivery and consumption is vital.

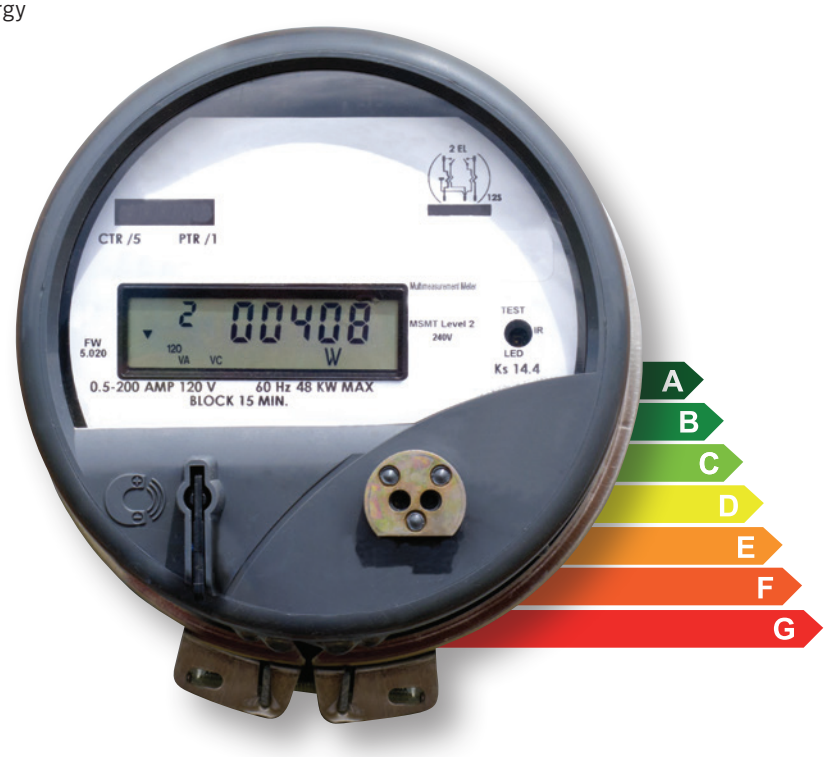
Smart grid technology aims to tailor the generation and supply of energy to user consumption, thus increasing efficiency, reducing costs and environmental impact. In particular, consumer 'smart meters' and sensors, equipped with IP addresses, can communicate information about energy utilisation patterns to the supplier, as well as allowing end-user control. This can help manage real-time demand, and even provide advice to consumers about usage habits.

Buildings, both residential and commercial, provide an important opportunity to optimise energy consumption and enhance the wellbeing of residents and workers. Intelligent buildings, particularly office environments, are able to leverage smart grid technologies to influence energy supply and consumption by controlling lighting, climate control and IT. They can even provide electric plug-in stations for employees to recharge their cars while at work.

Intelligent transportation

Keeping the city moving is critical. Transportation strategies have an impact on public safety, the environment, energy, rapid response services, the ability to do business, and critical deliveries; not to mention general quality of life.

Real-time traffic flow information, coupled with Telco, Global Positioning Systems (GPS), M2M communication, Wi-Fi and RFID technologies, as well as data analytics and prediction techniques, can be used to enhance private and public travel. Sensors can collect information about traffic conditions at critical city spots and send, via wireless or GPS communication, to centralised control systems. This data can then influence decision-making or even operate processes like traffic light synchronisation.



Connected healthcare

Healthcare delivery can benefit from a connected approach, with Electronic Patient Records available to all medical services. This will enable public health professionals and clinicians to collaboratively access information in a secure way, at any time, from anywhere and from any device.

In many cases, telemedicine solutions, connected through broadband, wireless or satellite, can prove vital in situations where the infrastructure or specific contingencies do not allow for the physical presence of a specialist – such as natural disasters or remote geographical locations.

An ageing population needs traditional care, but also assisted living and health monitoring services to enable independence at home. This can be achieved through the utilisation of sensors and devices connected to health operators through broadband, wireless and data analytics, and crucially, the deployment of privacy, identification and security systems.

Public safety and security

Above all, cities need to be safe. Public safety and security has become paramount for city administrations, whether protecting against crime, natural disasters, accidents or terrorism.

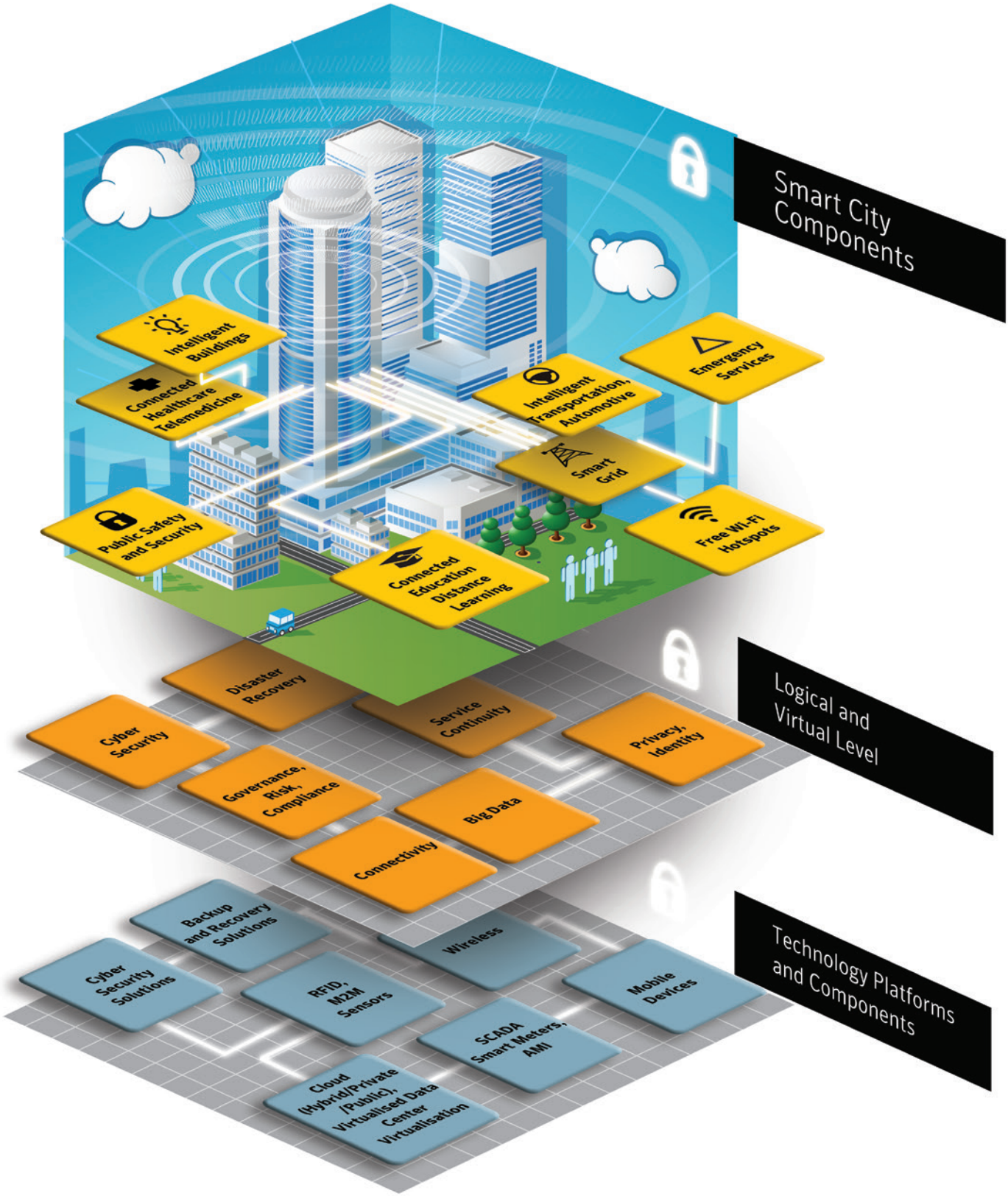
From conventional street violence to complex financial offences, identity thefts or data breaches, a dynamic crime horizon can only be tackled by increasingly sophisticated technologies and processes.

Telesurveillance systems are becoming increasingly pervasive in urban settings and, coupled with real-time communication capabilities, can help emergency services intervene promptly in incidents.

In the immediate aftermath of a serious accident or catastrophic event, the ability to share information between agencies, to operate sophisticated telesurveillance systems, to guarantee connectivity to incident response teams and first responders, to gather and analyse heterogeneous intelligence and data about incidents in real time, all in a reliable and secure way, allows municipalities and their emergency services to increase safety for citizens, businesses, assets and infrastructure.

Wireless communications and hotspots

Both large and small municipalities offer free wireless hotspots in addition to those provided by airports, hotels, and shops. As this trend is set to continue, given the popularity of the service, more and more citizens will be exposed to potential vulnerabilities; in particular the younger population who are at risk of being lured onto unsafe websites and chat rooms.


Smart City Components
Intelligent Buildings
Connected Healthcare Telemedicine
Intelligent Transportation, Automotive
Emergency Services
Smart Grid
Public Safety and Security
Free Wi-Fi Hotspots
Connected Education Distance Learning
Logical and Virtual Level
Disaster Recovery
Service Continuity
Cyber Security
Privacy, Identity
Governance, Risk, Compliance
Big Data
Connectivity
Technology Platforms and Components
Backup and Recovery Solutions
Wireless
Cyber Security Solutions
Mobile Devices
RFID, M2M Sensors
SCADA Smart Meters, AMI
Cloud (Hybrid/Private /Public), Virtualised Data Center Virtualisation

Ensuring continuity of critical services

The smart city aims to optimise quality of life by leveraging technology and integrating the different macro-functions discussed earlier. City governance should therefore ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy. In this scenario of overlapping functions, the process and information exchange in the city need to be interconnected and contextualised in a common middleware. The systems need to be standardised, interoperable and open but also secure; in order to take third-party information into consideration and ensure an overall seamless service delivery.

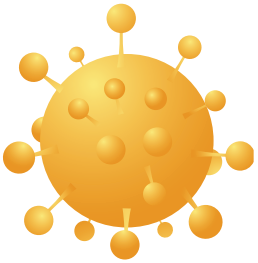
CIOs of local government are increasingly participating in strategic policy discussions and broader decisions on urban planning. Technology can enable the integration and the deployment of policies and support policy changes.

Like any other ICT system, the smart city technological and communication environment – the network infrastructure and the Internet of Things – will present vulnerabilities to cyber attacks. The higher complexity and heterogeneity of these environments could in fact determine an even higher exposure, and need for more sophisticated protection strategies.

Smart cities will need to factor in how deeply the city infrastructure and service life cycles will be impacted by their Internet of Things endpoint deployments. City department CIOs and CTOs must plan for security and functionality upgrades as well as bandwidth requirements (Gartner)[7].

The annual Symantec Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Global Intelligence Network, which Symantec's analysts use to identify, analyse, and provide commentary on, emerging trends in attacks, malicious code activity, phishing, and spam.

According to the 2013 **Symantec Internet Security Threat Report**,

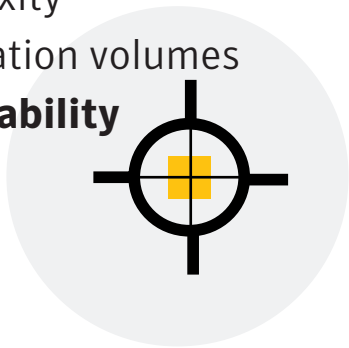


22% of targeted attacks are aimed at governments and energy/utilities companies, while governments and healthcare institutions are the target of **24%** of identity breaches[8].

Like any other ICT environment, cities can experience different types of cyber attacks. As systems grow more complex, become more interconnected and handle more information, their exposure to vulnerabilities increases; whether due to malicious intent or human error.

Administrations and their ecosystem of stakeholders in charge of designing, building, operating, maintaining and using the city and its services, need therefore to develop smart cities with security in mind from the conception stages.

Hyper connectivity
+ Hyper complexity
+ Hyper information volumes
= **Hyper vulnerability**



Given the impossibility of protecting every aspect of the ecosystem with the same level of sophistication and resources, choices will have to be made. City governance will need to identify the most critical areas to protect, the types of threat they could be subject to, categories of attackers and likely motivations (financial, criminal or political). City IT ecosystems will increasingly be built on public sector cloud or infrastructure virtualisation, with social and mobile computing as the primary access for applications and services.

In order to equip themselves for this transition and ensure the appropriate level of security and resilience of systems, cities will need to manage ICT leadership and governance, strong processes, people's mindsets and robust technology.

The right cyber security strategies can mean the difference between success and failure. The increasing urban deployment of public wireless networks, for instance, calls for robust security strategies to protect the Internet of Things connected through the city network.

Information management and protection systems and backup and recovery systems for mission-critical administration data should protect citizens' privacy and identities across domains, including local tax, healthcare, education and utilities.

When conceiving and building services, architectures and applications that leverage smart city information platforms, this should be done with high security against cyber attacks in mind, in order to guarantee service availability and continuity, data management and protection, as well as network resilience in case of severe incidents.

Open government data is also in great demand to promote transparency and citizen participation. Security and privacy are vital to protect citizens' identities and other sensitive government data.

Each of the functional systems presented above can attract interest from internal and external malicious attackers. They can attempt to compromise the delivery of services, or even provoke serious incidents, with potentially critical consequences, such as denial of critical services, network breakdown, or even fraudulent false information exchange.

By definition, vulnerabilities increase when systems become connected and integrated. In particular, this occurs when an unprecedented amount of additional data (Big Data) is generated by various smart devices (like sensors, meters and cameras) and processed by connected systems. The network infrastructure, be it broadband, Wi-Fi or satellite, that connects systems and their operators, adds entry points and opportunities for security breaches or human error.

For these reasons, it is important that smart city designers and planners develop solutions with robust, embedded cyber security and mitigation strategies in case of attack or loss of data.

Legislation is also becoming increasingly prescriptive in this domain. The Cyber Security Strategy of the European Union[9], published in February 2013, seeks to ensure that critical infrastructure is adequately protected from any kind of cyber attack, and that information is protected according to compliance standards.

Protecting the smart city's services

Securing the smart grid and critical infrastructure

Smart grids and related infrastructure need protection from attacks that could cause severe stoppages to cities, public communities, industrial sites and essential services.

Attackers exploiting vulnerabilities in SCADA systems (Supervisory Control and Data Acquisition), based on traditional software platforms, can lead to intrusions with the potential to disrupt data exchange between utility control centres and end users, and severely compromise the delivery of energy services. Whitelisting techniques, used to ensure that only specified system applications and processes are active at any one time, are particularly effective against zero-day vulnerabilities and attacks in SCADA environments. Zero-day vulnerabilities are still unknown on the day of the attack, hence they are vulnerabilities against which no vendor has released a patch yet.

Intruders can also install malware designed to obtain sensitive information, to control the networks that operate the service and cause a denial-of-service situation. This can be countered though intrusion prevention techniques, coupled with robust policies for areas such as network usage, browser patches, email and user awareness and education.

At end-user level, smart meters may simply be hacked and compromised for fraudulent purposes: to alter proof of consumption or to 'steal' energy from other users, while preventing the provider from detecting service flaws.

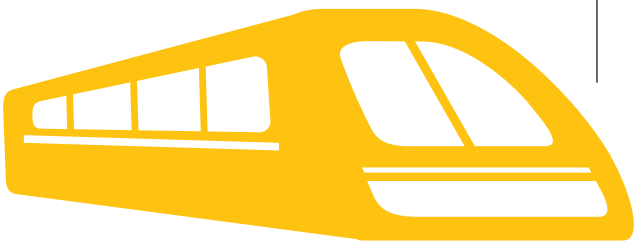
In order to make it impossible to manipulate smart meters in large scale and advanced metering infrastructures (AMIs), public key information (PKI) or managed PKI can be used, thus securing data integrity, revenue streams and service continuity.

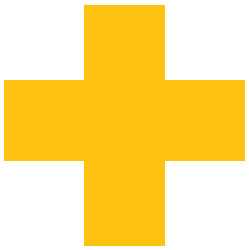
The smart grid can be secured at the communication layer by implementing PKI directly into meters, enabling identification, verification, validation and authentication of connected meters for network access. PKIs are ideal for large-scale security deployments requiring a high level of security with minimal impact on performance.

In a PKI environment, it is essential that private keys and certificates are guarded by a reliable management solution that protects against ever-evolving data threats.

The European Union project CRISALIS (CRitical Infrastructure Security AnaLysIS), for which Symantec is a project partner and coordinator, was launched in June 2012. Its goal is to provide new methodologies to secure critical infrastructure environments from targeted attacks, deliver new tools to detect intrusions, and develop new techniques to analyse successful intrusions[10].

The European Commission has also established a network of energy infrastructure operators. The Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) enables collaboration and common understanding between operators and governments, in order to contribute to the level of protection against external threats[11].





Optimising intelligent transportation

Optimising transportation models requires a high degree of complexity from the ICT infrastructure and its components to avoid disruptions. These can be the result of malicious intent or simply someone causing difficult conditions for pleasure. For example, traffic management could be impaired by hacking into the navigation system that directs a bus driver into the city through a wrong route, due to false information about traffic volume. Recently, a teenager in Europe was able to interfere with public transport control systems with a modified TV remote control, causing severe traffic disruption, including a tram derailment, by forcing a vehicle into a sudden turn at high speed[12].

The data transmitted from devices may be subject to spoofing. Unencrypted traffic data may be subject to attackers injecting false traffic reports into satellite navigation devices, as proven by cyber security experts. Vulnerabilities can also put information at risk due to unintentional actions, mistakes, carelessness or inadequate processes.

Protecting connected healthcare

Over the past three years, about 21 million patients in the US have had their medical records exposed in data security breaches[13].

In the case of a road accident, a malicious intrusion that compromises communication between first respondents and operational centres could prevent its correct localisation and the most efficient dispatch of emergency units. Equally, during such incidents, emergency services might need to operate using medical data for injured patients, by accessing a central location, and they should do so in the certainty of reliability and integrity of the information.

In this context, backup, cyber security and authentication solutions can ensure that healthcare systems offer such reliability and integrity, as well as patient privacy.

Maintaining public safety and security

It is critical that telesurveillance systems maintain their integrity and availability and that emergency services can rely on wireless or M2M communication to obtain directions and instructions from operational control centres.

Therefore, when information is transferred and managed over unsecured lines, between different operators, both internal and external, with heterogeneous systems, then data encryption is required. By leveraging strong two-factor authentication and one-time password entry, only trusted personnel can gain access to critical data and control systems. Digital certificates can also be used for authentication, signing and encryption.

Securing wireless communications and hotspots

Designing and building encryption solutions into devices ensures that they can only communicate with the required control centre and communications can be authenticated. It is critical that free Wi-Fi hotspots in cities, whether provided by private entities like shops or by the city administration itself, are secured. This helps to guarantee the safe handling of confidential information and personal data, such as usernames, passwords and credit card numbers. It also, crucially, helps to protect younger users via parental control techniques, which can prevent them from accessing inappropriate websites and being exposed to threats. This can be achieved by creating a secure, private, encrypted connection, undetectable to 'Wi-Fi sniffer' apps, making the user 'invisible' on public networks.

Safeguarding the connected smart city

The centralised governance body will ultimately run the smart city through a central virtual dashboard, comprising the ICT operational centre. This will need to provide ongoing assessment and timely response to varying incidents and needs. The reliability of services is at stake, and absolute continuity must be guaranteed.

Any threat to the security of the system and its information can be detected, analysed and dealt with using threat intelligence services. The ICT should be able to obtain reliable threat and vulnerability intelligence, and consequently dynamically adjust its security stance. In case of incidents, these need to be promptly and effectively managed by specialist operators and incident management tools in order to return users and services to their normal operational status. Comprehensive and expert managed security services are available in the industry for users to benefit from the providers' expertise and state-of-the-art solutions.

Recommendations for a secure transition to a resilient smart city

Smart cities can securely thrive and prosper if cyber security and information protection are fundamental components of the services provided to constituents. Critical steps and areas of focus should include:

Establishing the governance framework

Identify key stakeholders. Firstly, within the administration: the policy makers and their cabinets; the functional decision makers and heads of departments with their teams of expert civil servants; and the technical decision makers, CIOs, CISOs (Chief Information Security Officer), data center and network architects, administrators and developers. Secondly, within the overall ecosystem: citizens and their associations; the different constituents groups (taxpayers, motorists, public transport passengers, patients, hospital staff, pupils and students, school staff, office workers); physical infrastructure architects and developers and the emergency services.

Fulfilling Governance, Risk and Compliance (GRC)

This is a key consideration for public sector organisations, and can be fulfilled through policies and processes, enabled by ad hoc IT suites conceived to ensure that IT departments monitor their environment against the evolving regulation scenarios, and take appropriate action to stay compliant and mitigate risks.

Delivering service continuity

Cities should prioritise providers offering solutions and methodologies for security, backup, data loss prevention, archiving and disaster recovery, who are able to protect and manage heterogeneous environments resulting from legacy systems and newer deployments, including Open Source, managed mobile devices, and virtualised systems.

WEF: Cyber Resilience Maturity Model

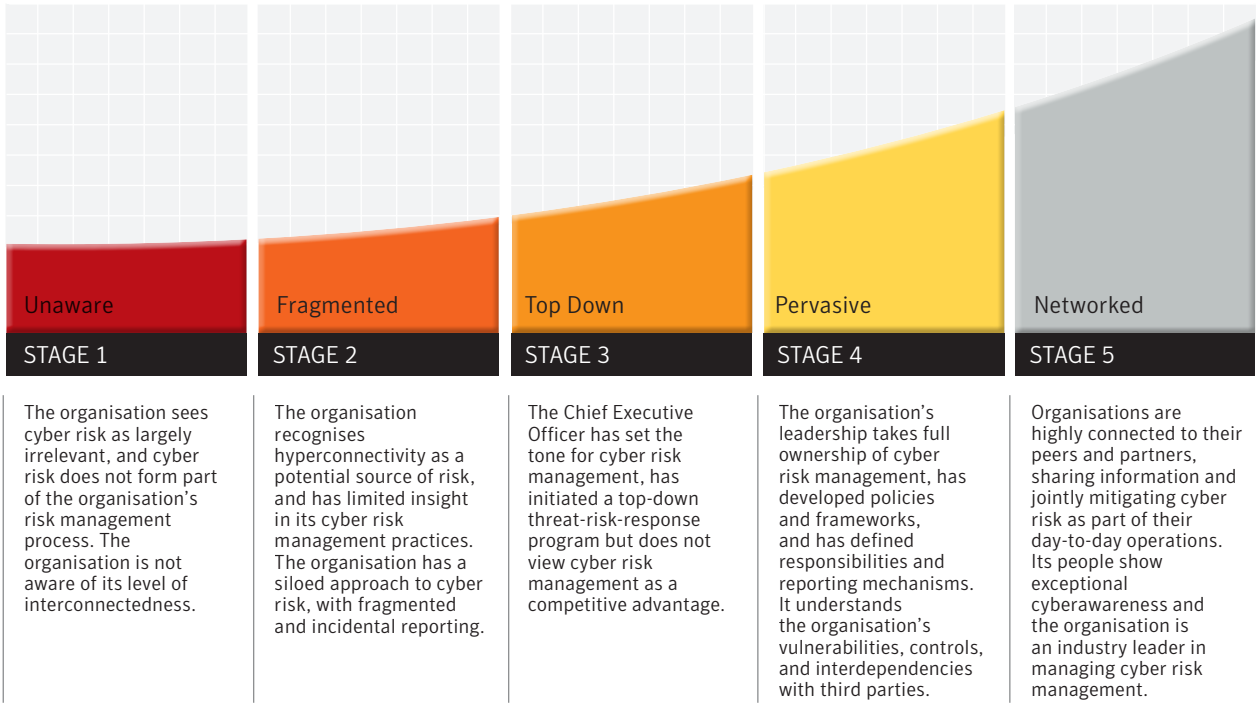


Figure 1: World Economic Forum Cyber Resilience Maturity Model[14]

Protecting information proactively

We have seen how this kind of smart city scenario involves Big Data considerations, and the need to centralise and manage the vast amount of information generated and used. Taking an information-centric approach, embedding security within data and taking a content-aware approach to protecting information is vital for identifying ownership of where sensitive details reside and who has access to them. Classifying data and utilising encryption helps to secure sensitive information and prohibit access by unauthorised individuals. Complex ICT infrastructure managing interconnected smart city services, can adopt protection leveraging host-based intrusion detection systems (HIDS) and host-based intrusion prevention systems (HIPS), as well as robust authentication policies and tools. This can help prevent any malicious intrusion attempts and the potentially devastating consequences for critical services.

Authenticating users

Strong authentication also enables organisations to protect public facing assets by ensuring the true identity of a smart device, system or application. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorised devices to the infrastructure.

Leveraging threat intelligence

In order to understand the major attack trends, city governance and CIOs can count on an established observatory, like the Symantec Global Intelligence Network, to provide one of the most extensive and accurate vendor-neutral analyses of trends on malware, security threats and vulnerabilities, from security research centres around the world. The same information is also used to compile the annual Symantec Internet Security Threat Report, which contains vital information about current and emerging threats and vulnerabilities.

Symantec Global Intelligence Network

The Symantec Global Intelligence Network collects the data upon which DeepSight Security Intelligence products are based. The Global Intelligence Network has global visibility into the threat landscape, including:

- *More than 64.6 million attack sensors monitoring networks.*
- *Over 45,000 vulnerabilities, covering over 15,000 vendors.*
- *Visibility into all ports/protocols for threat analysis and collection.*
- *More than 8 billion emails a day.*
- *More than 1.4 billion web requests a day.*

Balancing traditional versus cloud delivery

In a smart city environment, all the smart services mentioned so far can be delivered through a traditional client-server approach, but also through a cloud-computing model, in order to leverage 'as-a-service' capabilities and efficiencies.

Both private and hybrid cloud models require a secure virtualised environment, where data can be safely guarded and processed with appropriate Service Level Agreements (SLAs) to guarantee the essential services to citizens. Authentication and encryption policies and techniques can help ensure the integrity of the cloud environment and its safe function in the virtual space.

Availability and disaster recovery solutions should guarantee compliance with Service Level Agreements (SLAs) and resilience for critical city services.

Managing security services

Cities should also consider outsourcing security services to providers who can leverage extensive, global expertise in the field of cyber security to minimise security-related disruptions and data loss. The ICT leadership can then focus on the functional duties of running the city.

Cities should also rely on their national Computer Emergency Response Teams (CERT) to align with national coordination on cyber incidents and security and thus benefit from the international visibility this provides.

Protecting the infrastructure

Securing endpoints, messaging and web environments, defending critical internal servers and implementing the backup and recovery of data should be priorities. Organisations also need visibility and security intelligence to respond to threats rapidly.

24x7 availability of the critical infrastructure

Ensure resilience in case of an incident through solid backup and recovery software or appliances, policies, processes and tools.

Developing an information management strategy

This should include an information retention plan and policies. Organisations need to stop using backup for archiving and legal retention, and should instead implement deduplication everywhere to free up resources, use a full-featured archive and eDiscovery system and deploy data loss prevention technologies.

Cooperating with a security and information protection partner

Cities should choose a partner with worldwide visibility of threats and attacks trends, able to address the complete range of security challenges described in this report.

Conclusion

Smart cities are on the increase worldwide, and especially within Europe there are many initiatives stimulated by the EC and the national governments. Local administrators and policy makers will be increasingly driven to make their cities competitive in order to attract businesses, talent and taxpayers, and to comply with sustainable policies, greenhouse gas emission targets and carbon footprint guidelines.

Smart city deployments will involve multi-faceted developments, carried out by a diverse ecosystem of providers in innovative domains, involving state-of-the-art technology including critical and complex ICT implementations.

However, increasing ICT complexity will mean increasing vulnerability, both to malicious attacks and unintentional incidents. By conceiving interconnected urban systems with security and information protection in mind, city administrators will be able to ensure safety and wellbeing for citizens and businesses alike.

Security threats are now an integral consideration in the private sector boardroom, and for policy making within the public sector. Public administrators know that any serious incident or breach could result in devastating outcomes in terms of financial, data, credibility and reputation loss or damage.

Choosing reputable, experienced thought leaders as partners in conceiving such complex developments is an important step in the right direction towards building resilient smart cities for the twenty-first century.

References

1 Collins Dictionary Online, 'Resilience', Def. 2 http://www.collinsdictionary.com/dictionary/english/resilience

2 The US Presidential Policy Directive 21 (PPD-21): 'Critical Infrastructure Security and Resilience' http://www.dhs.gov/what-security-and-resilience

3 Information Security Forum, 'Cyber Security Strategies, Achieving Cyber Resilience', November 2011, p 14

4 World Economic Forum, Partnering for Cyber Resilience, 'Risk and Responsibility in a Hyperconnected World – Principles and Guidelines', March 2012, page 14 http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

5 Urban World: Cities and the Rise of the Consuming Class, 2012 http://gt2030.com/2012/07/17/urban-world-cities-and-the-rise-of-the-consuming-class/

6 Gartner, Inc., 'The Internet of Things Will Shape Smart Cities', Alfonso Velosa, March 28, 2013

7 Gartner, Inc., 'The Internet of Things Will Shape Smart Cities', Alfonso Velosa, March 28, 2013

8 2013 Symantec Internet Security Threat Report, pp.15 and 91 http://www.symantec.com/security_response/publications/threatreport.jsp?inid=us_ghp_thumbnail1_istr-2013

9 Cyber Security Strategy of the European Union http://europa.eu/rapid/press-release_IP-13-94_en.htm

10 CRitical Infrastructure Security AnaLysIS http://www.crisalis-project.eu/

11 Thematic Network on Critical Energy Infrastructure Protection http://ec.europa.eu/energy/infrastructure/critical_en.htm

12 The Register, 'Polish teen derails tram after hacking train network', John Leyden, 11 January 2008 http://www.theregister.co.uk/2008/01/11/tram_hack/

13 Computerworld, ''Wall of Shame' exposes 21M medical record breaches', Lucas Mearian, August 7, 2012 http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches

14 World Economic Forum, Partnering for Cyber Resilience, 'Risk and Responsibility in a Hyperconnected World – Principles and Guidelines', March 2012, page 12

Further reading

Healthcare Tech Review, 'OCR: 21 million patients have had protected health information breached', Scott Gibson, August 14, 2012 http://healthcaretechreview.com/ocr-21-million-patients-have-had-protected-health-information-breached/

Author

Giampiero Nanni, Symantec Corporation

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec is a global leader in providing security, storage and systems management solutions to help customers secure and manage their information and identities.