Symantec

We protect the world's people and information

CRITIS 2013

8TH INTERNATIONAL CONFERENCE ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY

SEPTEMBER 16-18, 2013, AMSTERDAM

Transformational Smart Cities: cyber security and resilience

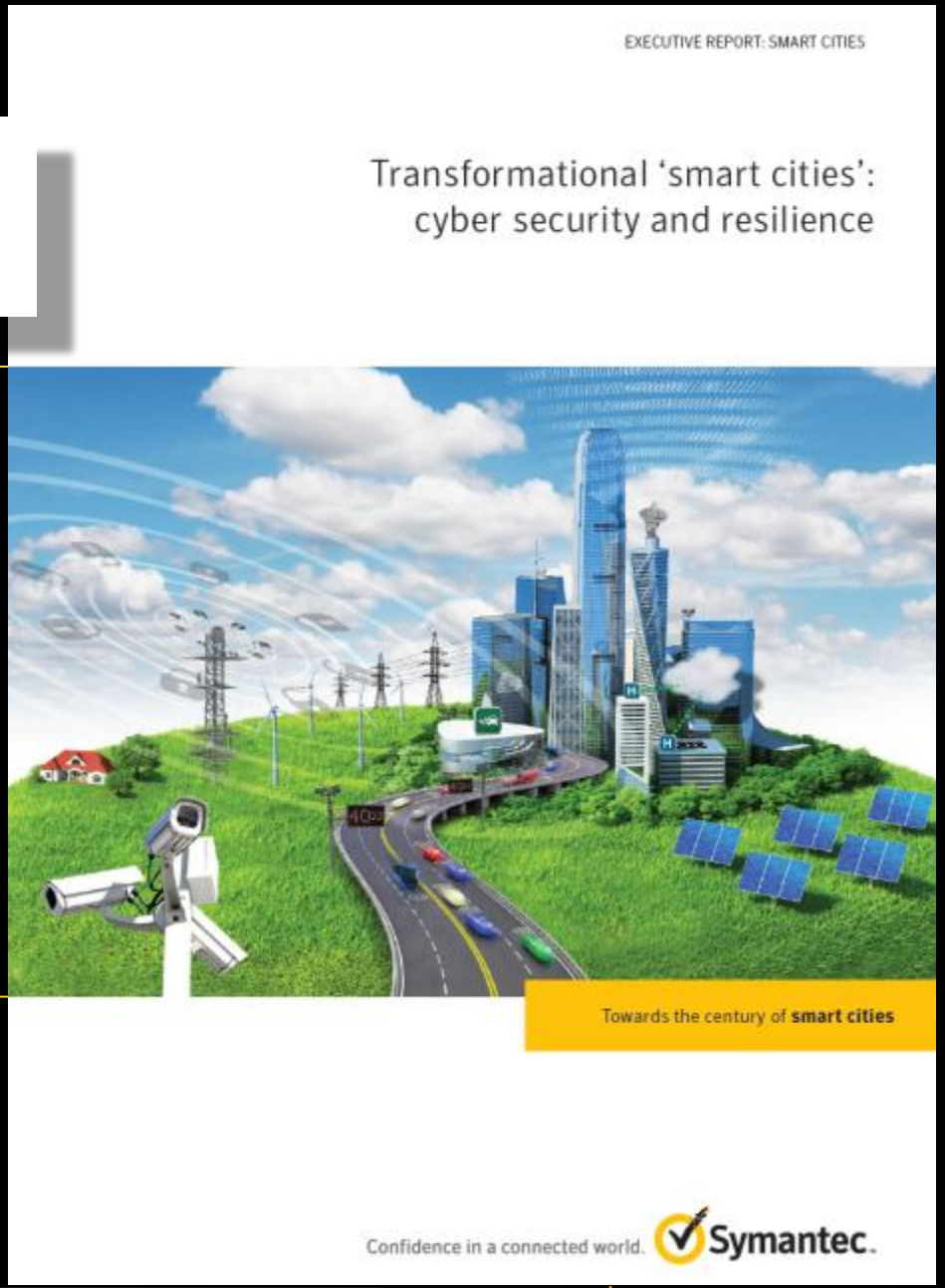
Towards the century of smart cities

Executive Report Overview

Giampiero Nanni

Public Sector Strategy EMEA, Symantec

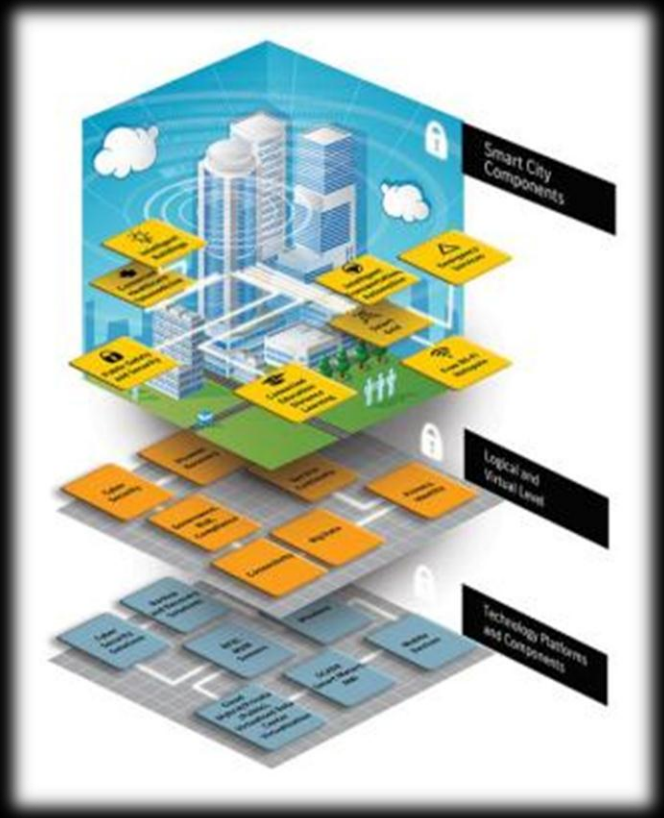
To obtain a softcopy of the report please go to http://bit.ly/106cTM8



Symantec

Highlights

- Urban challenges
- City competition: drivers & stakeholders
- Ensuring continuity of critical services
- Protecting the smart city's services
- Recommendations for a secure transition to a resilient smart city
- Conclusion
- Q&A



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.

“Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.”

Sun Tzu (The Art of War)

Connected smart city

- Smart Cities = ‘smart delivery of smart services’
- ICT as key enabler
- Highly complex ICT systems
- Highly interconnected components
- High volume of data

A resilient smart city…

…needs to be designed, from inception, with…

- Cyber security
- Privacy
- Integrity
- Compliance
- Reliability
- Resilience

…in mind

Urban challenges

- Delivering cost efficiency
- Eroded investments in services for citizens
- Population growth = Pressure on services quality
- Cities' role in carbon emission
- Energy requirements growth = pollution increase
- City congestion, efficient public transport
- Needs to protect critical infrastructure
- Ageing urban infrastructure
- Public safety and security
- More demanding citizens - 'Digital natives'

Definitions

Resilience: The ability of an ecosystem to return to its original state after being disturbed

(Collins Dictionary)

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)

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)

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)

World Economic Forum: Cyber resilience maturity model

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

City competition drivers

- " 'City 600' will generate nearly 65% of world economic growth until 2015" (McKinsey Global Institute)
- Modern cities compete with each other to attract businesses, talent, skills (and taxpayers)
- Businesses are attracted into cities by the ease of operation and quality of life for staff
- The smart city ecosystem is a broad public-private partnership

City stakeholders

- City Administration & its departments
- City planners and developers
- Research, Academia
- Energy and utility providers
- Automotive industry
- Facility control providers
- Non-governmental organisations
- IT system integrators, SW/HW vendors
- Technology providers → Mobile, Cloud, Networking, M2M, RFID, Cyber-security, etc.

The role of central Governments and the EU

- Cities' fortune is linked to their Region and Nation
- Benefit from Central Government's propulsion
- Glasgow, the UK smart-city champion: £24M Government fund
  - One-stop shop City dashboard , journey planning, traffic incidents, energy level monitoring, crime prevention, non-critical reports, hospital waiting-list info.
- The EU very active in the discipline with funds and projects

The integrated and interrelated smart city

The 'Internet of Things'

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".

'The Internet of Things Will Shape Smart Cities', Alfonso Velosa, March 28, 2013

"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)**

Smart city components

Smart city components

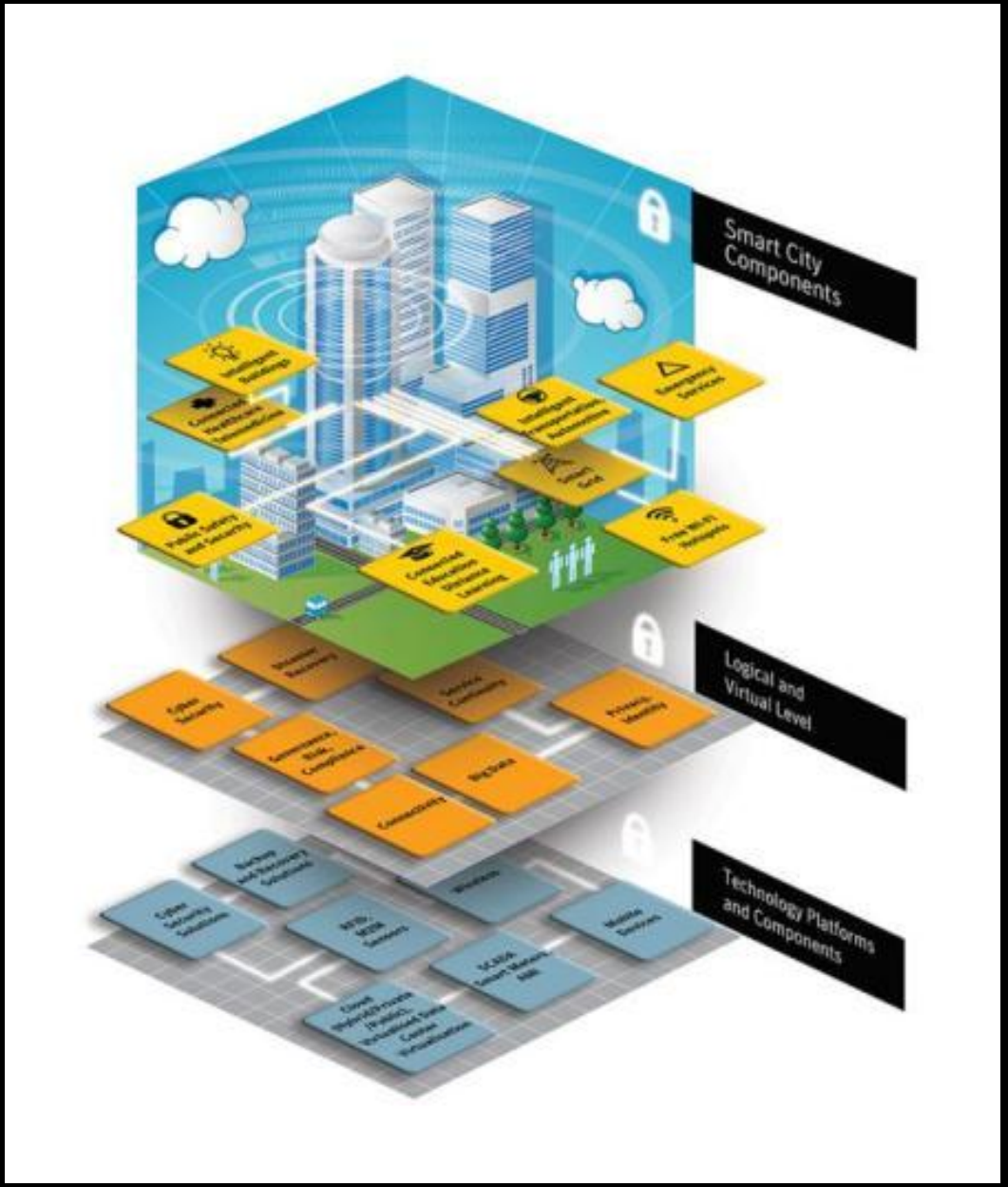
- Intelligent buildings
- Public Safety & Security
- Connected Healthcare, Telemedicine
- Connected Education, Distant Learning
- Free WiFi hotspots
- Emergency services
- Intelligent transportation
- Smart Grid

Logical & Virtual Level

- Cyber Security
- Governance, Risk, Compliance
- Connectivity
- Big Data
- Disaster recovery
- Privacy, Identity
- Service continuity

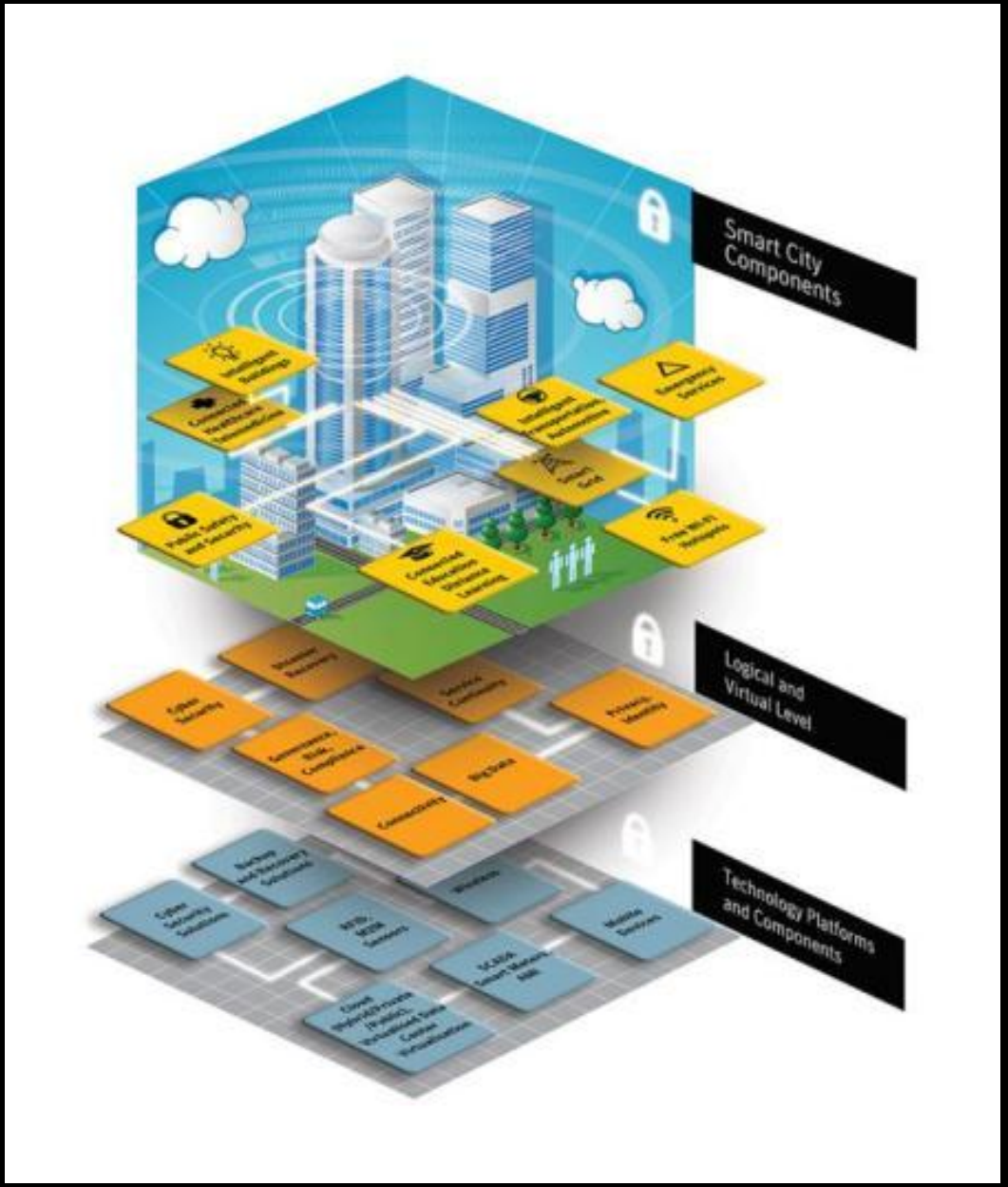
Technology platform and components

- Cyber Security solutions
- Backup and recovery solutions
- RFID, M2M, Sensors
- SCADA, Smart meters, AMI
- Mobile devices
- Wireless
- Cloud, Virtualised DC



Smart city components

- Smart grids and energy efficiency
- Intelligent transportation
- Connected healthcare
- Public safety & security
- Wireless & free hotspots
- ……

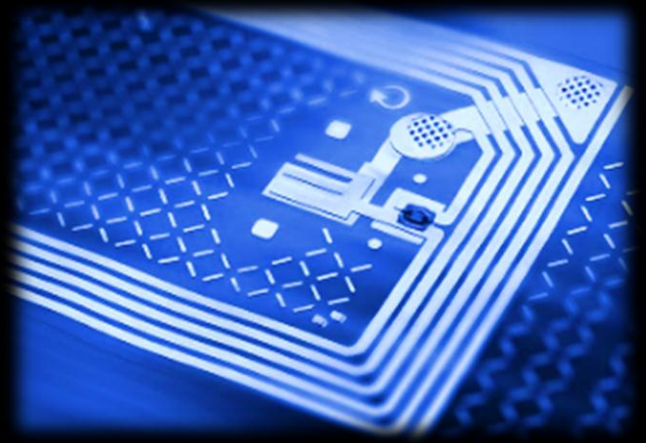


Smart grids and energy efficiency

- Cities consume between 60 and 80% of world's energy
- Smart Grid, smart metering with IP address and sensors allow monitoring and adjust generation and delivery based on consumption models
- Reduce cost and environmental impact

Intelligent transportation: keeping the city moving

- Real-time traffic flow information
- Telco, Global Positioning Systems (GPS)
- M2M communication, Wi-Fi and RFID technologies
- Data analytics and prediction techniques



Connected Healthcare

- Secure collaborative access for authorised medical services, to Electronic Patient Records, in a way, at any time, from anywhere, from any accredited device
- Telemedicine solutions for remote areas or in case of natural disaster
- Ageing population: assisted living and monitoring service for independence at home
- All require privacy, identification and cyber security

Public safety and security

- Protecting against crime, natural disasters, accidents or terrorism.
- Tele-surveillance systems to help emergency services
- First respondents to benefit from secure connectivity
- Secure data access and sharing

Wireless communications & hotspots

- Increasingly popular service, with increasing vulnerability
- Unsecure access to sensitive and personal data (online banking, social network, etc)
- Younger population particularly exposed
- Cyber-crime increasingly active in these environments

Ensuring continuity of critical services (1)

- City governance to ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy
- Technology to enable policy
- City CIOs increasingly part of strategic policy discussions

Ensuring continuity of critical services (2)

- Systems/IoT, need to be standardised, interoperable and open, but also secure
- Cyber-security and resilience to be embedded from inception
- Cyber-security + backup and recovery systems for mission-critical administration data
- Legislation increasingly prescriptive, nationally and EU

The EU

Cyber-security Strategy & Directive

of the European Union, 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

"Achieving cyber resilience"

Protecting the smart city's services

"He who defends everything defends nothing".

Frederick II of Prussia (The Great)

ISTR
INTERNET SECURITY THREAT REPORT ◆ 2013

Symantec Global Intelligence Network (GIN)

The Symantec Global Intelligence Network collects security data, and 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.

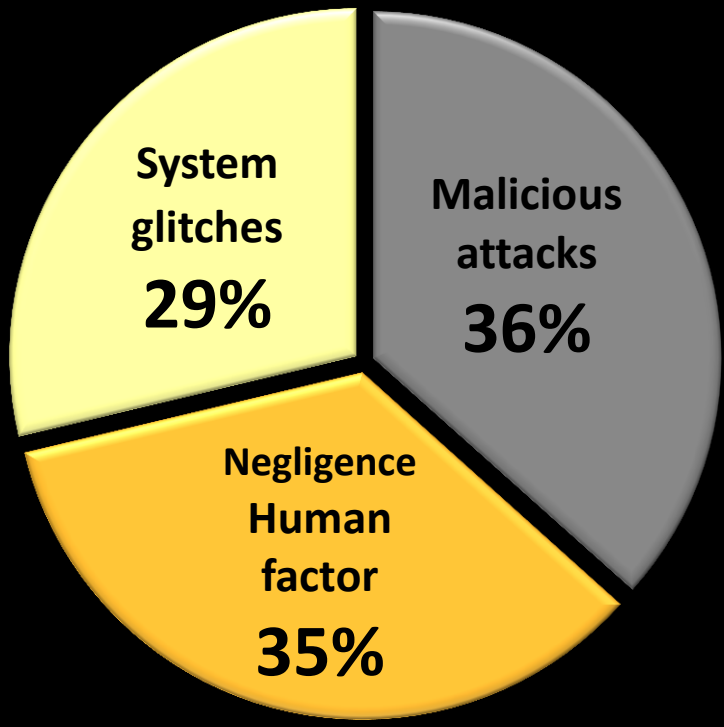
To access and download the full report please go to: ISTR 2013

- **%** of all email malware as URL: **23%**
- Overall email virus rate: **1 in 291**
- Overall email phishing rate: **1 in 414**
- Email spam/day: **30 billion** (69% of total emails)
- Web attacks blocked per day: **247,350 (90M+ per year)**
- Mobile malware families increase Y0Y: **58%**
- New unique malicious web domains: **74,000**
- Legitimate websites with unpatched vulnerabilities: **53%**
- Websites with critical vulnerabilities unpatched: **24%**
- Malicious web sites that are legitimate sites: **61%**
- Number of targeted attacks per day: **116 (40340/year), up 41% YoY**
- **%** of attacks on organisations by size: **2500+ employees: 50%. 250-2500, 19%. <250, 31%**
- Highest % of targeted attack recipients: **R&D 27%, Sales 24%, CEOs 17%**
- Top targeted attacks by industry: **Manufacturing 24%, FS 19%, Services 17%, Govt 12%**
- Highest % of Data Breaches per sector: **65% Govt/Edu/Healthcare**
- Top causes of data breaches: **40% Hackers, 23% Accidental, 23% Loss/Theft of equipment**

Recommendations:

- Assume You're a Target.
- Defense in Depth.
- Educate Employees.
- Data Loss Prevention.

Major causes of data breaches



- Negligence, human factor
  - Employee mishandling of confidential data
  - Violations of industry & government regulations
- System glitches
  - Lack of system controls
- Malicious attacks
- Average cost per capita (per record) of a data breach:
  USA $194, Denmark $191, France $159

"**2013 Cost of Data Breach Study: Global Analysis**"
by Symantec and the Ponemon Institute.

For more detail please go to: 2013 Cost of Data Breach Study

Measures to reduce the risk of data breach

- Educate people
- Put in place appropriate processes
- Use appropriate technology and tools (DLP)
- Use intelligence

Recommendations for a secure, resilient smart city… (1)

…in order to deliver service continuity and 24x7 availability of the critical infrastructure.

Establish the governance framework

- **Fulfil Governance, Risk and Compliance (GRC)**
- **Deliver Service Continuity**
- **Identify and protect vital information proactively**
- **Balancing traditional versus cloud delivery**
- **Authenticate users (Strong authentication)**
- **Manage security services**
- **Developing an information management strategy**

Recommendations for a secure, resilient smart city (2)

Fulfilling Governance, Risk and Compliance (GRC)

- Policies and processes, standards and regulations, enabled by ad hoc IT tools
- Ensure that IT departments monitor their environment against the evolving regulation scenarios
- Stay compliant and mitigate risks.

Delivering service continuity

- Adopt solutions and methodologies for security, backup, data loss prevention, archiving and disaster recovery
- Ensure 24x7 availability of the critical infrastructure and resilience in case of an incident through solid backup and recovery software or appliances, policies, processes and tools
- Able to protect and manage heterogeneous environments
- Legacy systems and newer deployments, Open Source, managed mobile devices, virtualised systems, etc.

Recommendations for a secure, resilient smart city (3)

Identify and protect vital information proactively

- Adopt an information-centric approach: embed security within data
- Encryption and white/black-listing
- Host-based Intrusion Detection Systems (HIDS) and Host-based Intrusion Prevention Systems (HIPS)
- Strong authentication policies and tools.

Balancing traditional versus cloud delivery

- Smart services delivered through traditional client-server approach, OR through a cloud-computing model (leverage aaS capabilities and efficiencies)
- Both private & hybrid cloud models require a secure virtualised environment
- Define appropriate Service Level Agreements (SLAs)
- 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 to guarantee compliance with SLAs, and resilience for critical city services.

Recommendations for a secure, resilient smart city (4)

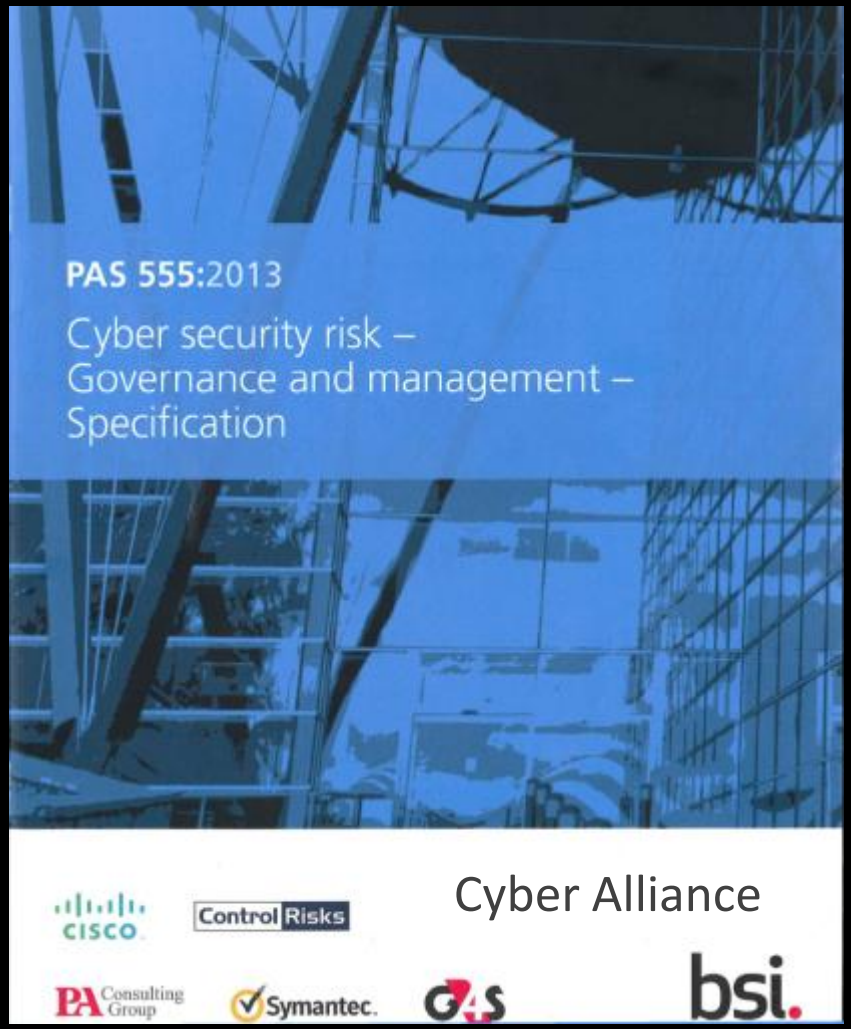
Managing security services

- Consider outsourcing security services to providers who can leverage extensive, global expertise in the field of cyber security
- 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.
- ICT leadership to focus on the functional duties of running the city
- Rely on national Computer Emergency Response Teams (CERT)

Developing an information management strategy

- Develop an information retention plan and policies
- e.g. “No backup for archiving and legal retention” - Instead implement deduplication, use archive and eDiscovery system, deploy data loss prevention technologies (DLP)

PAS 555 – An 'Outcome-based' specification



This PAS is intended to be used as a stand-alone specification, or it can be used as a companion to other relevant standards, by any organization that wishes to have confidence in its cyber security.

The requirements of this PAS define the overall outcomes of effective cyber security. These outcomes can be achieved in a variety of ways, which are not specified here. However Annex A provides an illustration of how other relevant standards can deliver the requirements of this PAS. It should be noted, however, that the list in Annex A is not exhaustive or prescriptive and there may be other standards which are more specific to an organization's business.

The PAS specifically targets top management of an organization and intentionally has broad coverage in terms of its requirements. It does not intend to replace existing, well-established standards but provides a potential framework for understanding the outcomes of other standards in a specific cyber security context.

Conclusion

Smart city deployments imply vulnerability

- Diverse stakeholders
- State-of-the-art technology and capabilities
- Complex, heterogeneous ICT implementations
- Hyper-connectivity, IoT
- Big Data

Cyber-attacks and data breaches are costly

- Data loss
- Financial loss
- Reputation and credibility loss

Conceive the resilient smart city with cyber-security in mind

- Organise processes
- Educate people
- Acquire intelligence
- Equip with appropriate tools

TO ACCESS AND DOWNLOAD THE FULL REPORT PLEASE GO TO:
SMART CITY EXECUTIVE REPORT

To obtain a softcopy of the report please go to http://bit.ly/106cTM8 or contact me directly

Thank you!

Giampiero Nanni

Public Sector Strategy – EMEA, Symantec

giampiero_nanni@symantec.com