

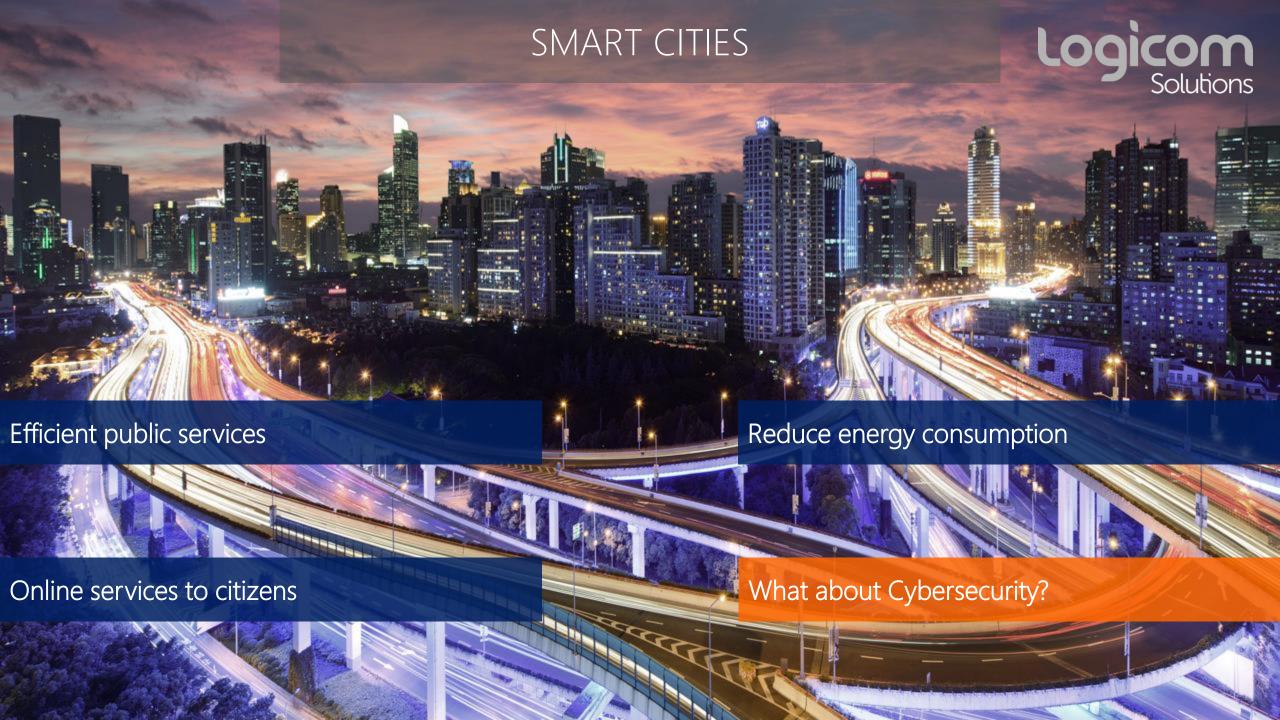
CYBERSECURITY CANNOT BE AN AFTERTHOUGHT

IN OUR SMART CITY JOURNEY



Smart Cities Event – Logicom Solutions June 2022















DIFFERENT THREAT ACTORS

The threat actors are changing to online fraudsters



ATTACK SURFACE IS CHANGING

New services and channels are being introduced which can be targeted



NO PHYSICAL CONSTRAINTS

A city can be targeted from anywhere, from everyone.



AGAINST WELL ORGANIZED GROUPS

It's not only individuals. Sophisticated and well organized groups are the major threat.



THE MOST INFAMOUS HACKING GROUPS



LAZARUS HACKING GROUP



SILENCE HACKING GROUP



CODOSO HACKING GROUP



CARBANAK HACKING GROUP













MORE THAN 100 HACKING GROUPS



BUSINESS CONSULTING SERVICES

Smart City Services that can be targeted



Logicom Solutions



SMART TRAFFIC CONTROL

Security review of the newly developed banking systems and infrastructure.



CCTVs - CAMERAS

Traffic and surveillance cameras can allow attackers to spy or make cities blind.



MANAGEMENT SYSTEMS

Attacks targeting the different internal systems to cause impact on the operations.



SMART GRID

Attacks against the smart grid can result in a black-out.



SENSORS

To send fake data and affect how automated decisions are made (e.g. Raise alerts, panic).



STREET LIGHTING

Compromise the street lighting system to take control and turn on-off the lights.



SMART TRANSPORTATION

Display incorrect information, cause delays and overcrowding.



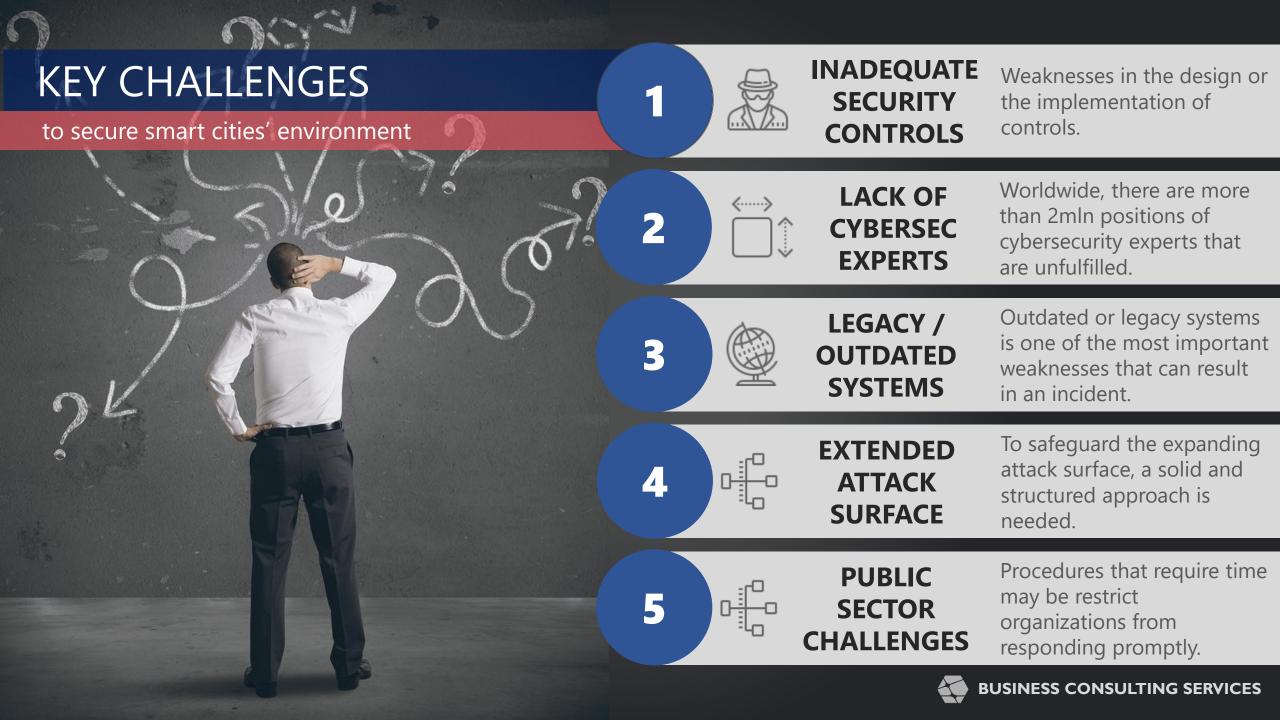
SOCIAL MEDIA

Comprised social media accounts and posting of fake news or notifications to cause confusion.



PUBLIC DATA

The crown jewels of every organization. Exfiltrate sensitive data is always a key objective.





NATIONAL SECURITY NATIONAL ECONOMY SOCIAL WELLBEING

HEALTH AND SAFETY

ENVIRONMENT



PERFORM RISK ASSESSMENTS

Assess your risks, identify threats and evaluate the effectiveness of your controls and prepare your risk treatment plan.

CONDUCT PENETRATION TESTS

Simulate hackers' activities to identify the possible entry points to your environment or services.

INCIDENT RESPONSE PLANS

Be prepared to respond to an incident and to recover the operations in the event of a successful cyberattack.

SECURITY AWARENESS

Run a continuous security awareness programme. Human factor is still the weakest link in the security chain.

Logicom Solutions



CHARIS FLORIDES
CISSP, OSCP, MSc in InfoSec



Division Head, Business Consulting Services **Logicom Solutions**



Board Member

ISC2 Cyprus Chapter



email address
c.florides@logicom.net



Linkedin Profile charis.florides

