CHAPTER 160 SWITZERLAND

Workshop Smart Cities

Basel 15.09.2015 - Geneva 16.09.2015

Rev. 1.1 – 11.02.2016

Content

1 Workshop objectives

ASIS International, Chapter 160 Switzerland has identified the topic of **sustainable, resilient and smart cities as a core topic for the security profession** and for the security industry.

Today 4 billion people - 54% of the world population - live in cities, and every week another 1'000'000 people migrate into cities. Cities produce more than 75% of the world's GDP, but also more than 75% of the world's challenges, such as energy consumption, traffic of people and goods, carbon gas emissions, … and crimes.

Systems put in place to cope with these challenges are increasingly interconnected and hence increasingly vulnerable. Although energy consumption, transportation and interconnectivity issues are in the focus of city managers, the aspects of safety and security and hence sustainability for critical infrastructure, citizens and business are by and large underestimated and insufficiently addressed.

As a community of security professionals, ASIS International, Chapter 160 Switzerland has therefore taken the initiative to identify safety and security related issues and to inform the relevant stakeholders about the challenges at hand. The primary objective of the workshops held in Basel and Geneva was therefore to **gather input from national and international experts on the issues at hand and to identify first avenues for solutions to the challenges**.

It is particularly important to realize that Smart Cities is not about implementing smart technology, but about providing smart solutions, smart living conditions and a smart operational environment to citizens – as individuals but also as economic players in enterprises or institutions.

2 Participants

2.1 Speakers

The following people were invited to provide a keynote address before the workshop discussions (in alphabetical order):

- Ian Abbott, director Security, Safeguards, Safety and Environment for the UK Nuclear Decommissioning Authority
- Dino Auciello, journalist (moderator)
- André Duvillard, delegate of the Swiss Security Network
- Marc Henauer, head of the Swiss Operations and Information Centre MELANI - reporting and analysis centre for information assurance (deputy in Basel: Stefan Glaus)
- Roman Lehman, regional manager and crisis communication officer, Protectas SA

- Thomas Romig, chief airport steering at Geneva airport
- Peter Siebert, Smart City project manager Berlin

2.2 Workshop participants

Including the speakers the Basel event was attended by approx. 20 participants, the Geneva event by approx. 35 participants. In both locations participants came from public institutions, from enterprises looking for a safe and secure business environment, and from safety and security providers / consultants.

3 Program

3.1 Overall program

Following key note addresses and a question & answer session on the core topics, the participants split in 4 groups to first discuss each core topic and then to report to the plenary.

3.2 Focus Topic 1: Smart cities

- What is a smart city?
- What is at stakes at local and national level?
- Which are the security challenges posed by smart cities?
- What are the major risks and how to explain their impact to stakeholders in the private and public sectors and to the public?
- How to develop standards and best practices based on a holistic approach?

3.3 Focus Topic 2: Critical infrastructure

- Which roles critical infrastructures play in a smart city?
- What are the risks to critical infrastructures and their impact on private businesses?
- How to protect business activities?
- How to tackle the conjunction between physical and cyber risks?

3.4 Focus topic 3: Business continuity and emergency management

- What role can the private sector play?
- Do smart cities generate new types of risk?
- What types of crises are specific to smart cities?
- How to learn from past experiences?

3.5 Focus topic 4: Public-private partnerships for safety and security

- Should private and public security resources be shared?
- What would be the advantages of sharing resources?
- Which resources to share and how?
- What are the examples of resource sharing and how to learn from them?

4 Key note addresses

4.1 Ian Abbott, UK Nuclear Decommissioning Authority

"Being smart does not mean the city will be incident free."

Whether malicious, accidental or naturally occurring incidents will require effective management by visible and available senior people, be they elected politicians or chief executives: the most senior person of any organization has to be on the incident scene whereas the ongoing business can be managed by the 2nd in charge.

Crisis management leaders and emergency services need to develop and continuously update a common, trusted and coherent view of the incident at hand as a basis for proactively dealing with the issues. This obviously requires a plan and communication means in place in order to gather key people and to collect information in a structured manner at the outset of the incident as well as whilst measures to cope with it unfold. The primary objective is to maintain public trust in words and deeds in order to ensure a willingly compliant attitude of the public towards issued instructions and requests.

It is essential to have well known and trusted individuals at the forefront of the crisis leadership team who are able to unite people concerned and to display real empathy for those involved.

Prepared plans must allow for scaling up of command and control arrangements and resources in a flexible manner, all the way to international coordination, depending on the scale of the incident. Plans should include robust public private partnerships in order to deploy resources beyond those of the entity immediately concerned by the incident – regular rehearsals being a key ingredient to success.

The stress levels caused by serious incidents need to be considered to develop mental and psychological strength for crisis management leaders and key staff: most of the challenge is about soft elements and people – not the hard technology.

Therefore it is best to avoid thinking in scenarios, but to rather train for dealing with disruptive events on the basis of incidents that actually happened – in your organization or anywhere else. Experience can be systematically developed and further enhanced by extending known incidents in time, magnitude or scope.

4.2 Peter Siebert, Smart City Berlin

"In 2030, Berlin will be a prototype for urban life in the 21st century, an intelligently networked, sustainable, post-fossil and resilient city for the benefit of an educated, tolerant and creative society."

Berlin's distinctive features are a high level of dynamics and a unique urban culture. High quality of life, open-mindedness and citizen-oriented politics make Berlin very attractive for the best talents from all over the world. The city is characterized by close cooperation between business and science on the basis of solid infrastructure and environmental protection. Thus, it creates optimal location factors for entrepreneurs and researchers who also benefit from innovative types of financing, fast decision-making and efficient processes.

Berlin is a role model for continuous transformation of an intelligent city which manifests itself at many future locations and where the citizens and their needs are the center of all action. Having room for diversity, experiments and innovative technologies, the German capital's central feature will particularly remain one thing: unique.

The focus of the Berlin Smart City initiative is about creating and maintaining a highly competitive urban environment to attract talent and businesses. Smart public safety and security is a key ingredient to such an objective and hence a key component of the Berlin Smart City Strategy with "new security concepts":

- Start with top-down commitment
- Qualify leaders and define responsibilities for dealing with challenges and crises
- Adjust plans to constantly changing and transforming leaders and cities
- Develop plans to include and integrate internal and external resources
- Create "safety and security controlling" to monitor ability to deal with challenges
- Design procedures to make use of existing security systems infrastructure
- Manage big data versus privacy issues
- Particularly focus on dealing with infrastructure disruptions
- "Copy/edit/paste": cooperate with other cities

4.3 André Duvillard, Swiss Security Network

"An emergency situation may require management and ability to act through several months with scarce key resources such as staff, food, electric power, information & communication, fuel, cash or logistics."

Based on article 57 of the Swiss Constitution, the Swiss Security Network (SSN) has the mandate to coordinate efforts at all levels to "ensure the security of the country and the protection of the population."

The basis of the SSN action is a global preparedness approach including all major risks resulting from main drivers such as demographic change & urbanization, in-

formation density & complexity, mobility, international interdependence, privatization, and individualism. Preparedness has to include private actors such as food suppliers & distributors, financial institutions, information & telecommunication players and private security providers. In Switzerland the levels of the federal system have to be considered: Confederation, cantons and municipalities.

The identified key ingredients so far include private security service providers with more than 1000 enterprises and more than 16'000 employees and the not yet identified players in cyber security. It is essential to establish private public partnerships to ensure the resilience of the entire society.

4.4 Roman Lehman, Protectas SA

Private Public Partnerships (PPP) will be seriously challenged in times of crisis: private partners will be resource constrained due to the need to protect their own operational staff and the need to serve their regular customers."

Whilst there is no doubt that risk concentration increases due to the increasing interconnection and interdependence, public resources that can deal with incidents and emergency situation decrease as a result of limited budgets. For a Smart City the disruption of critical infrastructure (payment systems, power supply, communication systems, mobility, etc.) is the single most important risk as it will transmit consequences to the entire society.

Preparedness for PPP means a paradigm shift from passive solutions to active solutions that are permanently engaged and can be ramped up at short notice (such as the Swiss Humanitarian Aid Unit). The private service providers would expect a compensation for their preparedness, i.e. for adequate training of staff and for defined guarantees of availability in case of crisis.

4.5 Marc Henauer, Reporting & Analysis Centre for Information Assurance

"I think we all find it comfortable if our refrigerators re-order milk in the future, … but it might be disturbing of the milk starts ordering refrigerators after a hack attack." (cited from Evelyne Widmer-Schlumpf, Federal Councilor, 2008-2015)

The Reporting & Analysis Centre for Information Assurance of the Swiss Confederation has the mission to protect private users of home computers, small and medium-size enterprises and critical infrastructure operators from trouble and disruptions caused by cyber attacks.

It defines risk by the equation: **R = V * T * I**, whereby:

R = risk
V = vulnerability, technical and non-technical, taking into account degree of integration and interconnectivity

T = threat, based on global and integral assessment
I = impact, expressed in magnitude of business or societal consequences, taking into account degree of interdependency between citizens, enterprises and infrastructure

In Smart Cities vulnerability and impact increase due to the high level of interconnectivity and of remote operation – independently of threat level. This holds in particular for critical infrastructures which are essential for the working of the economy and of the society.

When dealing with complex entities such as Smart Cities it is essential to conduct an overall risk management based on the definition above, including organizational and people related issues as opposed to a purely technology focused view of IT security.

4.6 Thomas Romig, Geneva Airport

"Emergency Management and Business Continuity Management is about minimizing the impact of disruptions on customers and operations"

Emergency Management is based on 4 key pillars:
- Risk identification
- Preparedness
- Response
- Recovery

Crisis management covers the period from the disruptive event through the response and into recovery, based on standards processes, procedures and systems developed during the preparedness phase.

Business continuity deals with maintaining the continuity of operations during the crisis (even if at reduced output and/or higher cost) as well as ramping up for the recovery of normal operations.

Crisis management and business continuity management are two distinct activities that have to be handled by different parts of the organization (see also Ian Abbott's comment on crisis handling vs. running the ongoing operations).

After a disruptive event – whether in real life or in an exercise situation – an evaluation of the performance in crisis management and business continuity management has to be conducted in order to define improvement measures for the preparedness phase.

5 Report of workshop sessions

5.1 Basel and Geneva workshops

For each of the focus topics discussed in Basel and Geneva this section contains the aggregated findings and outcome of discussions.

5.2 Focus Topic 1: Smart cities

- What is a smart city?
- What is at stakes at local and national level?
- Which are the security challenges posed by smart cities?
- What are the major risks and how to explain their impact to stakeholders in the private and public sectors and to the public?
- How to develop standards and best practices based on a holistic approach?

Cities are designed for the citizens as private people but also as members of a society with economical, political, cultural and social interactions. Smart cities have to provide efficiency and comfort to be livable and attractive for citizens. They always have to respond the citizens' question: "what's in it for me?" Explicitly or implicitly the Smart City has to make itself understandable and to raise awareness for the consistent quality of its services. At the same time the stakeholders (individual citizens, businesses, political decision makers, public institutions, administration, etc.) have to feel understood and be an active contributor to ensure their needs are adequately reflected.

The coordination of the stakeholder's needs and interests calls for an active leadership. Leaders have to incorporate the various cultures in the different parts of the city into an aggregated smart culture in their speech and deeds, a result of the various cultures. Therefore they need to obtain and share information, to learn how to extract the common interest from the various stakeholders, learn how to obtain agreement on common interest and objectives.

Putting people first – before technology – is essential. Communication, trust and transparency are key ingredients.

From a safety and security perspective the common interest is "peace of mind" as a basis for a comfortable and prosperous private and economical life in a sustainable manner. To make sure this common interest is strongly included in the Smart City planning and development it is recommended to "personalize" through a senior city official, such as a **Resilience Officer** (RO). The role of the RO is to make sure that long-term safety and security needs are taken into account in all dealings of the Smart City. The RO can base his action on:

- Interaction with the stakeholders, but also
- Exchange of knowhow with peers in other Smart Cities
- KPI's measured according to ISO 37120 (which includes 100 Global City Indicators, thereof 11 focused on safety and security)

According to research conducted be the Rockefeller Foundation 100 Resilient Cities program, City Resilience is the capacity of individuals, communities, institutions, businesses, and systems within a city to survive and grow no matter what kinds of chronic stress and acute shocks they experience.

The biggest challenges to create the role of a Resilience Officer is to start the dialogue and get the sponsor – who must be the most senior officer of the city, i.e. the mayor! Despite serious disruptive events in particular in relation to terrorism there still is a fairly widespread perception of limited threat level. To create awareness, position the mindset and make available budgets for a Resilience Officer, a "burning platform" must be developed, either a serious disruptive event in the own city, or a major disruptive event in another comparable city (e.g. flooding, black-out, terrorist attack, a major cyber hack). This requires an understanding of a common objective for safety and security and may be pushed by a united stakeholder alliance.

5.3 Focus Topic 2: Critical infrastructure

- Which roles critical infrastructures play in a smart city?
- What are the risks to critical infrastructures and their impact on private businesses?
- How to protect business activities?
- How to tackle the conjunction between physical and cyber risks?

Increasing complexity and interconnectivity create by themselves increasing vulnerability and threat levels. On the other hand increasing interconnectivity also can be used to enhance resilience in the form of redundant systems if critical single points of failure can be avoided. Reducing vulnerability is not only a technical issue to be resolved at systems level, but to a large extent a matter of people and processes. Often the relevance and ownership of information is not sufficiently well understood.

Recommendations for dealing with the vulnerability:

- There is a need for decisions on political level for the identification of critical infrastructure with subsequent regulatory measures in relation to safety, security and resilience
- The identification process shall lead to a comprehensive list of critical infrastructure operators (within the federal system of Switzerland with a clear allocation of responsibilities to national, cantonal and local levels)
- The management of the vulnerability of critical infrastructure should in no case be left to private owners without an adequate regulatory framework
- The political level shall formulate targets, resilience levels, and monitoring principles; the critical infrastructure operators design and implement the measures.
- The regulatory aspects in particular have to cover the crisis management structures and responsibilities as well as the role and accountability of private owners.
- The regulators have to devote special attention to the ICT side: cyber security from a systems and processes point of view

5.4 Focus topic 3: Business continuity and emergency management

- What role can the private sector play?
- Do smart cities generate new types of risk?
- What types of crises are specific to smart cities?
- How to learn from past experiences?

The private sector clearly understands the need for business continuity and emergence management based on its genuine interest for survival of the enterprise. However unless a formal regulatory framework defines priorities and targets in a binding manner, each private enterprise will define their own objectives, possibly without alignment. It is therefore essential to also bring “business” continuity and emergency management to the political level: in a complex smart city, the ability to deal with chronic stress and with acute shocks depends on the capability of all stakeholders to recover and improve in a commonly coordinated manner – even if based on subsidiarity of the players.

Modern societies are no longer homogeneous. Therefore, emergency management should follow a bottom-up approach as opposed to a traditional top-down approach. An important issue is to determine how trust can be established amongst individuals and at local level. In a crisis situation, the question will be: “can I trust my neighbor?”

It is essential to obtain a detailed understanding of all critical processes to better implement resilience. People at all levels should be involved so as to identify essential players even at the lowest social or hierarchical level.

A silo mentality must be avoided and business continuity plans should be shared. To achieve this, concerns about security of information should be addressed in priority in order to reassure all stakeholders that sensitive information will be handled appropriately.

The risk appetite of smart cities stakeholders should be determined at commercial, political and individual levels.

5.5 Focus topic 4: Public-private partnerships for safety and security

- Should private and public security resources be shared?
- What would be the advantages of sharing resources?
- Which resources to share and how?
- What are the examples of resource sharing and how to learn from them?

A collaboration between private security service providers and public law enforcement is a reality – though still at fairly low acceptance on a political level and from the leadership of public law enforcement. We are “in the middle of the bridge”, i.e. collaboration is there but it is not yet fully accepted.

Based on the outcome of a crisis management exercise back in 2014, the Swiss Security Network clearly favors a significant enhancement and improvement of public-private partnerships. This is all the more important as many critical infrastructure and key resources, such as communication networks, food warehouses and logistics chains, petrol stations, or power production are largely or even fully operated by the private sector: a public-private partnership for resilience includes much more than the cooperation between law enforcement and private security service providers.

6 Conclusions and next steps

6.1 Conclusions

Given identified vulnerabilities and threats there is no doubt that Safety, Security and Resilience have to be integral parts of any city development concept in order to qualify as smart. Due to the pressing needs in energy, mobility and ICT there is a serious risk that safety, security and resilience aspects are overlooked – or at least managed at a lower priority level.

As a community of safety and security experts, ASIS International – Chapter Switzerland feels the need to highlight the safety, security and resilience topic on the political agenda of Swiss cities.

6.2 Next steps

- ASIS International – Chapter 160 Switzerland will create an ad-hoc working group on “Safe, Secure and Resilient Smart Cities”. Workshop participants and other interested parties are welcome to join and can apply for membership in the WG by mail to rolf.sigg@outlook.com.
- In 2016 the WG will first develop a white paper to facilitate the creation of a “burning platform” for Swiss cities.
- Based on the white paper the WG aims at engaging at least one Swiss city into a “pilot project” for a safe, secure and resilient Swiss Smart City.