D5.3

CYBERSECURITY AWARENESS IN MUNICIPALITIES

The story of the CS-AWARE project

Grant Agreement number:	740723
Project acronym:	CS-AWARE
Project title:	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis

Principal author:	Jerry Andriessen, Wise & Munro, jerry@wisemunro.eu
Co-editors and reviewers	Thomas Schaberreiter, University of Vienna; Juha Röning. University of Oulu; Alex Papanikolaou, InnoSec
Other authors:	Gerald Quirchmayr, University of Vienna; Chris Wills, Caris Research; Kim Gammelgaard, Rheasoft; Thanasis Poultsidis, Larissa; Massimo Ferrarelli, Arianna Bertollini, Omar Parente, Claudio Ferilli, Roma Capitale; John Forrester, Manolo Leiva, Massimo Della Valentina, Cesviter.

Document version: 1.0

Table of Contents

Executive Summary

In this Deliverable we present an overview of the CS-AWARE project. It is conceived as a potential book publication, written for stakeholders in public administrations and professional companies, and it comprises 6 chapters. In Chapter 1, we provide an introduction to the current cybersecurity landscape, both in a global sense and mapped to the specific requirements of LPAs. We identify a gap in the current state-of-the-art with respect to awareness and collaboration to improve cybersecurity in LPAs - and its relation to the current European cybersecurity framework - and we outline the requirements for closing that gap. The chapter is concluded by pinpointing how CS-AWARE addresses those requirements and giving an outlook on how the following chapters detail the respective solutions. In Chapter 2, we explore the background of the approach to systems and dependency analysis (SDA) that we used for the two pilot cities. Beginning with an overview of the inception and development of the current understanding of the importance and significance of the nature of socio-technical systems, we then describe the approach we took to conduct the SDA's in the pilot cities and describe the results that we obtained. We conclude with a review and discussion of our overwhelmingly positive experience of using SSM in a cybersecurity setting. In Chapter 3, we focus on the technological aspects of the implementation of the CS-AWARE solution, which aims at supporting system administrators with cybersecurity awareness about the information system they are in charge of, by analysing the information found in the log files of their most critical systems and visualising the results in an appropriate manner. In this way, system administrators are quickly informed whether there are indications of suspicious activity occurring in their systems and they also receive recommendations or suggested actions to take for specific instances of the aforementioned issues. Furthermore, by collecting and analysing publicly-available cyberthreat intelligence, the CS-AWARE system is able to deduce whether there are cyberthreats in the wild that could harm a specific information system it monitors and issue the necessary warnings accordingly. In Chapter 4, we present the viewpoint of the users of the CS-AWARE technology, the pilot municipalities of Rome and Larissa. Users address their motivations, their objectives, and their expectations for the CS-AWARE system. Crucially, we present the main impacts of their participation in this project: increased reflection, increased understanding of their own context and system, increased teambuilding and collaboration, and collaboration with academy. In Chapter 5, we discuss the complexity of marketing CS-AWARE to the public sector. CS-AWARE is not a concrete product to sell, as in: here it is, there you have it. It is explained that the public sector is complicated, and heterogeneous in many aspects: size, policies, degree of autonomy and cooperation. Policy agents in smaller municipalities often lack the relevant knowledge, lack sufficient funding, and often have no explicit policy. For our context, we should link to the needs and expectations of potential customers. This asks for building good relationships and credibility. Various tactics for building up understanding and rapport are presented, including educational ones. Finally, in Chapter 6, we summarise the outcomes of the CS-AWARE intervention in two municipalities. Because we collected their feedback during most of the design and implementation processes, users are strongly involved and have a sense of ownership. We discuss the ‘awareness’ concept in some detail, to conclude that many aspects of awareness have been evolving in a positive direction. We end the chapter with a short discussion of two domains for which our approach to cybersecurity awareness could also make a positive contribution.

Introduction

Jerry Andriessen, Thomas Schaberreiter, Alex Papanikolaou and Juha Röning

In this Deliverable we present, in a descriptive style, the story of the CS-AWARE project, addressed to the target audience of LPA cybersecurity stakeholders: policy makers in municipalities and regional/ national entities, persons involved in technological management, system administrators, amongst others.

In the CS-AWARE project we propose a cybersecurity situational awareness solution for local public administrations that, based on an analysis of the context, provides automatic incident detection and visualization, and enables information exchange with relevant national and EU level authorities involved in legislation and network security.

Cybersecurity is one of today's most challenging security problems for commercial companies, NGOs, governmental institutions as well as individuals. Reaching beyond the technology focused boundaries of classical information technology (IT) security, cybersecurity includes organizational and behavioural aspects of IT systems and needs to comply to legal and regulatory framework for cybersecurity. For example, the European Union recently passed the Network and Information Security (NIS) directive that obliges member states to get in line with the EU strategy. While large corporations might have the resources to follow those developments and bring their IT infrastructure and services in line with the requirements, the burden for smaller organizations like local public administrations will be substantial and the required resources might not be available. New and innovative solutions that will help local public administration to ease the burden of being in line with cybersecurity requirements are needed. For example, cooperation and coordination is one of the major aspects of the NIS and EU cybersecurity strategy. An enabling technology for cooperation and coordination is cyber situational awareness and information sharing of cyber incidents, both within an organization and with relevant actors outside the organization. Advanced features like system self-healing based on the situational awareness technologies, and multi-lingual semantics support to account for language barriers in the EU context, are part of the CS-AWARE solution.

The core concepts of this project, and of this deliverable, are ‘cybersecurity’ and ‘awareness’. It should be noted at the beginning that these are fuzzy concepts. First, ‘cybersecurity’ is a qualification belonging to a particular context, in our case, local public administrations. Because we explicitly include this context into our approach, and this context is characteristically subjected to ongoing fluctuations in local policies, knowledge, people and resources, what is considered a ‘secure’ technological environment differs between contexts. Second, new threats to this security, coming from the inside and the outside, develop all the time. Hence, what is secure at one moment, may not be secure at the next. The same applies to the software that is exploited for a secure environment. Also, legal and regulatory frameworks evolve, so meeting legal requirements is an ongoing effort. There are more reasons, but we stop here, hoping that it is clear to the reader that cybersecurity is not an all-or-none condition. For the project, this means that the users of cybersecurity technology always have to relate to their local context and the particular situation, for example, of how they detect a particular cybersecurity event. This takes us to the second main concept, which is ‘awareness’.

The fuzziness also applies to ‘awareness’. As we will see in the chapters of this deliverable, awareness can be understood from several viewpoints. It is a ‘psychological’ concept, which

means it does not exist materially, neither does it have precisely defined boundaries. It is a concept that has both human and technological aspects, and these aspects interact, i.e. mutually influence each other. We have tried to grasp the extension of this concept in an empirical setting (in real life) in another deliverable (D5.1, page 16) as involving knowledge and agency. The knowledge of cybersecurity awareness includes (1) knowledge about threats, (2) knowledge of the local system network, its components and the business processes involved, (3) knowledge about the organisation itself and the users (e.g. professionals within the organisation, and the citizens outside of the organisation), and (4) knowledge about the cybersecurity community (e.g. in other municipalities, legal and regional authorities, international expertise). Agency refers to the ability or willingness to act, in case of cyber incidents, but also when there is no incident, as in regular monitoring policies or maintenance of safety regulations. In all contributions to this deliverable we will address many components of cybersecurity, and our users will explicitly address the changes in awareness that they have observed by their participation in the project. We will see how cooperation and collaboration within the organization and with external cybersecurity actors helps to bridge this knowledge gap to achieve better cybersecurity awareness and thus the facility to better address cybersecurity problems within the organization.

This deliverable has 6 chapters, which together comprise the story of CS-AWARE. It is our aim for readers to get a clear idea about our proposal for cybersecurity awareness in municipalities, what we did to build our solution, and what was the impact of this work, including the voices of our users in all phases of the design, deployment and evaluation of the technology, and of their own cybersecurity awareness.

In Chapter 1, we provide an introduction to the current cybersecurity landscape, both in a global sense and mapped to the specific requirements of LPAs. We identify a gap in the current state-of-the-art with respect to awareness and collaboration to improve cybersecurity in LPAs - and its relation to the current European cybersecurity framework - and we outline the requirements for closing that gap. The chapter is concluded by pinpointing how CS-AWARE addresses those requirements and giving an outlook on how the following chapters detail the respective solutions.

In Chapter 2, we explore the background of the approach to systems and dependency analysis (SDA) that we used for the two pilot cities. Beginning with an overview of the inception and development of the current understanding of the importance and significance of the nature of socio-technical systems, before moving onto a description of the Soft Systems Methodology. We then describe the approach we took to conduct the SDA's in the pilot cities and describe the results that we obtained. We conclude with a review and discussion of our overwhelmingly positive experience of using SSM in a cybersecurity setting.

In Chapter 3, we focus on the technological aspects regarding the implementation of the CS-AWARE solution, which aims at supporting system administrators with cybersecurity awareness about the information system they are in charge of, by analysing the information found in the log files of their most critical systems and visualising the results in an appropriate manner. In this way, system administrators are quickly informed whether there are indications of suspicious activity occurring in their systems and they also receive recommendations or suggested actions to take for specific instances of the aforementioned issues. As a result, system administrators do not need to spend time analysing and correlating potential indicators to form

an opinion on the cybersecurity status of their systems. Furthermore, by collecting and analysing publicly-available cyberthreat intelligence, the CS-AWARE system is able to deduce whether there are cyberthreats in the wild that could harm a specific information system it monitors and issue the necessary warnings accordingly.

In Chapter 4, we present the viewpoint of the users of the CS-AWARE technology, the pilot municipalities of Rome and Larissa. This viewpoint has in part been elicited through stories and workshops, and in part is directly written as text of this chapter. Users address their motivations, their objectives, their expectations for the CS-AWARE system. Crucially, we present the main impacts of their participation in this project: increased reflection, increased understanding of their own context and system, increased teambuilding and collaboration, and collaboration with academy.

In Chapter 5, we discuss the complexity of marketing CS-AWARE to the public sector. CS-AWARE is not a concrete product to sell, as in: here it is, there you have it. It is explained that the public sector is complicated, and heterogeneous in many aspects: size, policies, degree of autonomy and cooperation. Policy agents in smaller municipalities often lack the relevant knowledge, lack sufficient funding, and often have no explicit policy. For our context, we should link to the needs and expectations of potential customers. This asks for building good relationships and credibility. Various tactics for building up understanding and rapport are presented, including educational ones.

Finally, in Chapter 6, we summarise the outcomes of the CS-AWARE intervention in two municipalities. Because we collected their feedback during most of the design and implementation processes, users are strongly involved and have a sense of ownership. We discuss the ‘awareness’ concept in some detail, to conclude that many aspects of awareness have been evolving in a positive direction. We end the chapter with a short discussion of two domains for which our approach to cybersecurity awareness could also make a positive contribution.

1 A case for cybersecurity awareness systems

Thomas Schaberreiter, Gerald Quirchmayr, Alexandros Papanikolaou

1.1 Introduction

In this Chapter we present an introduction to the increasingly challenging topic of cybersecurity in general, and the specific case of cybersecurity in local public administrations (LPAs). We outline the current cybersecurity landscape, as framed by recent European advances in cybersecurity law and regulation like the EU cybersecurity strategy, the network and information security directive (NIS) and the general data protection regulation (GDPR). Furthermore, an analysis of current trends in the global cybersecurity threat landscape is provided, and we give an overview of the currently available cybersecurity solutions for organizations on the technological, organizational and trans-organizational (national, European and global) collaborative level. We discuss the advantages/disadvantages of each solution and we will argue that all of those elements fulfil an important role, but in order to adequately protect the data managed by LPAs, a more holistic, socio-technical approach that is built upon cybersecurity awareness and collaboration in the organizational context is required.

We discuss the relevance of the European and global cybersecurity environment for the specific context of local public administrations and the and applicability of different approaches. Our analysis has shown that the data which is managed by LPAs (both citizen services and organizational services) are the most critical asset to be protected. We will outline the importance of protecting this data through the entire information flow caused by the day-to-day operations and processes of an LPA workflow. Following up on those aspects, we show how cybersecurity awareness in the organizational context can bring additional and novel elements to the existing state-of-the-art solutions, and which concepts, methods and methodologies are required to implement such a solution. The core concept includes continuous monitoring of system elements through dynamic, data driven risk and incident management. This requires the introduction of intelligent data analysis systems to provide accurate and context specific monitoring results and awareness. Furthermore, in order to fully utilize the advantages of cybersecurity awareness, the organizational culture needs to shift as well, from seeing cybersecurity as an individual or IT department task, to seeing cybersecurity as a collaborative socio-technical effort that requires the contribution of each individual in the organization - supported by a technological platform that allows this collaboration. Finally, we illustrate how good cybersecurity awareness in an organization lays the foundations for more advanced features like system self-healing (awareness of a problem is the basis for automated implementation of prevention or mitigation mechanisms) and cybersecurity information sharing (exact determination of the cause of an incident through awareness allows to determine information to be shared with cybersecurity communities for collaborative cybersecurity efforts, or in the context of mandated incident sharing requirements, as for example imposed by NIS or GDPR).

1.2 The cybersecurity landscape

Over the past decades we have seen a steady rise in both system vulnerabilities, and in attacks exploiting them. These unfortunate developments are well-documented by ENISA (ENISA

2019) and EUROPOL (IOCTA 2011-2019) in their cyber threat reports. Accordingly, the European Union has in its 2013 Cyber Security Strategy set the frame for a coordinated strategic approach to addressing the issue (EU CS 2013). The currently most important legislative cornerstones based on this strategy are the GDPR (GDPR 2016) and the NIS directive (NIS 2016), both of them having a significant impact on the perception of the importance of cyber security for European society, infrastructure and economy. Recent information operations aimed at destabilizing institutions and organizations are documented by The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE 2017).

While targeted attacks on Local Public Administrations (LPAs) are still the exception, the danger of an LPAs infrastructure being used as backdoor for intruding more important governmental systems is very real (COMPACT 2018). As research on supply chain security shows, this type of threat keeps increasing (Lamba 2017) and becomes especially relevant for LPAs that manage critical (information) infrastructures. While ransomware attacks in 2017 (WannaCry 2017) have increased the awareness for this problem, the threats posed by malware, DDos and APT attacks still tend to be underestimated. With IoT devices now becoming omnipresent, LPAs can easily become collateral damage in attacks that get out of control or that are launched in a massive way against potentially ill-defended targets of opportunity to exploit unpatched systems suffering from unattended vulnerabilities. These attacks have in the past caused and continue to cause large-scale impacts in an organization if this vulnerability is present. The embarrassingly clear reason for an attack being successful is all too often outdated software (due to limited resources) or unpatched software due to unawareness of update practices or slower response times in update practices due to resource limitations. Seen against the background of the current 2019 IOCTA (Internet Organised Crime Threat Assessment) report, the potentially devastating consequences of such negligence become evident (IOCTA 2019, pp.8,9):

- Ransomware remains the top cyber threat in 2019, and phishing and vulnerable software (especially vulnerable remote desktop protocols) remain the main infection vectors.
- Data is the key target for cybercrime.
- There is a growing concern in organizations about sabotage, for example by destructive ransomware.
- A growing need for collaboration between network and information security efforts and law enforcement is identified.

With the value of data managed by LPAs becoming an increasingly important asset, the probability of attacks raises continuously and it may therefore not be a question of “if”, but rather of “when” an attack occurs. Consequently, in LPAs the impacts of such attacks need to be limited to protect the managed data. This is best achieved through an awareness system that monitors relevant high-value assets for security relevant parameters like outdated software components or unusual behaviour that would indicate an attack. As past cases have shown (RUAG 2016), one of the major challenges is the early warning against and the early detection of vulnerabilities, related exploits and ultimately attacks launched against an LPA. In such an environment, keeping an up to date situational awareness picture of an LPAs cyber infrastructure becomes a high priority. To achieve this, a more user centric approach is required

that allows LPAs to be aware of their systems security state and the state of the data managed by those systems at all times, but at the same time facilitates collaboration between actors within the organization (like management, IT, service users), but also actors from outside the organization like NIS authorities or law enforcement. The remainder of this Chapter will outline the current state-of-the-art cybersecurity mechanisms at the disposal of LPAs to ensure cybersecurity, and we will identify the gap in the current state-of-the-art that needs to be addressed in order to achieve a collaborative approach to cybersecurity based on cybersecurity awareness in LPAs.

1.3 The state-of-the-art in cybersecurity practice

Digital and web-based technologies have transformed the way citizens can interact with LPAs, by facilitating the provision of electronic and remote services. In this way, citizens can be served more quickly and in a more efficient manner, since some of their requests can be processed without having to physically go to the LPA. Nevertheless, the provision of such services, as well as the involved data (both in transit and at rest) require a sufficient level of protection against cyberattacks, since a single breach can affect the data of many citizens, which usually is of significant sensitivity. In the remainder of this Section, various solutions for protecting LPAs will be presented, from different perspectives (technological, organisational, national/European/global).

1.3.1 Technological

When it comes to adequately protecting an LPA against cyberthreats, it is necessary that certain security mechanisms are installed so that a satisfactory cybersecurity protection level can be achieved. Firstly, a perimeter defence must be set up, which serves as the first line of defence. The primary security mechanism used for this purpose is a firewall that essentially divides the network into internal (trusted) and external (untrusted) sections and monitors the network traffic flows between them. Through the firewall's rules the organisation's security policy is implemented and according to them the communication requests are allowed or dropped.

Should remote connectivity for external users be required, the use of a Virtual Private Network (VPN) is usually applied. External users connect to the firewall and authenticate themselves. Once this process is completed, a secure connection between the external user's device (e.g. computer) and the organisation's firewall is established, the so-called VPN, which grants the authenticated user access to the organisation's internal network.

The internal network also requires a sufficient degree of protection, to both prevent e.g. malware infections from happening and prevent them from spreading across the whole internal network in the unfortunate case that they manage to bypass the installed security mechanisms. For instance, a user looking for something on the Internet may unintentionally initiate a malware download to the local computer, thus creating the initial infection, that may spread to the rest of the network if there is no mechanism to contain it. This kind of protection is usually offered via endpoint protection software, which consists of a collection of antivirus, firewall and access control features (e.g. permitting the connection of USB storage devices or not).

Once the aforementioned security mechanisms have been installed, it is equally important to monitor the activity in the organisation's information system, aiming to detect any suspicious behaviour as soon as possible and consequently react promptly to deal with the detected issue.

A popular mechanism for performing such a task is an Intrusion Detection/Prevention System (IDS/IPS), which monitors the network traffic at designated points of the organisation's network, analyses the traffic and detects potentially suspicious behaviour, according to the rules that have been set to it. An IPS usually interacts with a firewall, so that it can react to a detected threat (e.g. block the source IP address of the detected suspicious traffic).

A security mechanism similar to the IDS/IPS is a SIEM system (Security Information and Event Management). Their main difference is that the IDS/IPS monitors network traffic, whereas the SIEM analyses in real time the activities in an IT environment (namely, log files that contain information about various events happening at key network nodes). Any detected abnormal activity raises an alert, which has to be further investigated by the system administrator to determine whether this may be an indicator of a cyberattack taking place (e.g. too many user log-in failures may be due to a password-guessing attack).

Nevertheless, both IDS/IPS and SIEM solutions require administrators to monitor the alerts they produce and look into the involved issues. In several cases investigating the issue may require significant time and cybersecurity expertise that the majority of system administrators may not have. For this reason there is a trend for organisations to outsource their network security services to a Managed Security Services (MSS) provider, who offers 24/7 monitoring and response by their team of cybersecurity experts. Of course a 24/7 service has quite a significant cost associated with it, which does not make it a very attractive option for small organisations with a tight budget.

1.3.2 Organisational

Installing security mechanisms is not enough for achieving a high cybersecurity level, especially as the size and the complexity of an organisation increases. Organisational risk management is the process of identifying, assessing and controlling threats, which contributes to the enhancement of its cybersecurity level. The most important assets are initially identified, together with applicable threats to them and suitable controls are put in place to keep the calculated impact of a potential mishap as low as possible.

The need for organisational measures is also covered by the well-established family of the ISO27000 standard that involves the security of an organisation's information systems. Compliance to this standard (certified by appropriate certifications obtained via audits) implies that suitable procedures have been put in place to conduct information security management according to the best practices.

Common Criteria (CC1 2017; CC2 2017; CC3 2017) is a certification through which computer systems users can specify their security functional requirements (SFR) and security functional assurance requirements (SARs) using protection profiles (PP). Technology vendors can then hire testing laboratories to evaluate their products to determine whether they meet the said requirements. The European Agency for cybersecurity, ENISA, has recently published the candidate version for a European certification scheme (EUCC 2020) to cope with up-to-date cybersecurity requirements.

Nevertheless, using security standards in an organisation has certain drawbacks that in some cases may render the implementation of such a standard not worthwhile. To start with, they require significant expertise and familiarisation for both implementing and maintaining them,

which effectively translates into a need for significant additional resources. This includes the training required for familiarising the personnel with the newly-introduced procedures, as well as the ongoing training for creating awareness. Furthermore, the various procedures that will be introduced as part of the standard's implementation will impose an additional overhead to the existing daily activities. It may therefore not be practical for relatively small organisations, as they are lacking resources to handle this extra overhead. The financial aspects should also be considered too, as the implementation of such standards may require special equipment that would have not been bought otherwise, or that has to meet certain specifications and is therefore more costly than lower-level alternatives. What is more, the cost of obtaining and maintaining a relevant certification should also be considered.

1.3.3 National, European and global cybersecurity efforts

At the European level, the EU Cybersecurity Strategy (EU CS 2013) suggests a series of actions to enhance the cyber resilience of IT systems, reduce cybercrime and strengthen EU international cyber security policy and cyber defence. The cybersecurity strategy states that Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) are responsible for coordinating and supporting the response to a computer security event or incident. They exist at national, European and international level, and they communicate hierarchically so as to maximise their effectiveness in cybersecurity protection.

The legal and regulatory frameworks are also to be considered. For instance, in Europe, the GDPR (GDPR 2016) has quite recently come into effect, a European Regulation for unifying the protection and privacy of EU citizens' data. In order to achieve compliance with the GDPR both technical and organisational measures need to be utilised. Once a satisfactory level of compliance has been achieved, the organisation's cybersecurity level is also improved.

The NIS Directive (NIS 2016) also aims to boost the overall level of cybersecurity in the EU. At national level it requires Member States to have national CSIRTs, perform cyber exercises etc. to achieve and maintain a high cybersecurity level. It also emphasises on the need for cross-border collaboration between EU countries, through their CSIRT network and other competent groups and task forces. Finally, it requires Member States to supervise their critical infrastructure sectors (energy, transport, water, health, digital infrastructure and finance) and adequately protect it against cyberthreats.

Such a supervision can be performed by suitable cybersecurity mechanisms (e.g. SIEM) that will be installed in the organisation's information system. There are cases where such critical infrastructure services are controlled by LPAs or lie within the competency of a larger LPA. Hence, monitoring of such infrastructures will certainly help in creating cybersecurity awareness, as system administrators will be informed about detected cyberthreats that previously used to go unnoticed. What is more, the information about such cyberthreats could further be exploited by being forwarded to competent CERTs/CSIRTs and therefore promote cybersecurity awareness at a national and/or European level.

1.4 Cybersecurity requirements for LPAs

Like any organisation of a certain complexity, LPAs vary significantly in their individual set-up and the socio-technical interrelations that evolve naturally guided by organizational culture and policies. Looking at it from the European perspective, the set-up and structure of LPAs is

also heavily influenced by national legislations, so there are significant national differences in how LPAs operate based on the governing framework that defines the responsibilities and obligations of LPAs. All of those aspects influence the cybersecurity, and need to be taken into account when devising cybersecurity solutions. While based on those environmental conditions it becomes clear that a definitive and generalizable characterization of cybersecurity requirements for LPAs seems unrealistic, this Section will give a guiding overview of how IT systems are usually involved in providing administrative services to citizens and businesses in its constituency - and what this means for cybersecurity. In the following Section we will show how the individual socio-technical organizational differences are a crucial aspect in cybersecurity considerations, and how CS-AWARE was designed to be able to embrace this fact and provide cybersecurity solutions tailored to individual organizational cybersecurity needs.

There are two general distinctions in IT services operated within LPAs: 1) Services that are offered to citizens and 2) services to manage operations within the LPA. The first category includes simple services that are offered to inform citizens, like the web page or keeping and providing public records, as well as complex e-government services that allow to interact citizens or organizations with the LPA, for example to apply for permits. Most of those complex services map to strictly defined business processes that are not completely automated and require back-office handling and approvals, often by several individual departments in the LPA. The second category includes the more standardized organizational administrative operations, like for example human resources (HR) and payroll systems. While both service categories, when looking at them strictly from the technological standpoint, follow similar implementation and deployment patterns, there are two relevant distinctions that are important from the cybersecurity perspective: First, the data managed by the services in each category is fundamentally different in the sense that one category only manages and processes data (both sensitive and personal data) of employees, while the in the other category potentially sensitive and/or personal data about every citizen is managed and processed, and a breach in those systems would potentially leak a significantly larger amount of data. The second major distinction is in the potential complexity of business processes that are the basis for the offered service. While organizational management usually follows fairly standard organizational practices not unique to LPAs, IT based or IT supported administrative services for citizens may require the implementation of complex processes, often following the same policies and procedures implemented for the off-line counterpart - including integrated processes where IT only supports parts of the process like communication and data gathering, while the processing is still carried out as a back-office task. In terms of cybersecurity, this increases the potential attack points and thus the requirements in cybersecurity.

One additional trend that could be observed in recent years is the continuing centralization of services that traditionally have been the responsibility of LPAs, but due to the advantages of digitalization can now be managed directly at the national level. One good example for this is the citizen registry, which has - especially in European countries - traditionally been a local or regional responsibility, but is now increasingly managed as central register. From the cybersecurity perspective, this development reduces the burden on LPAs to provide adequate protection for the services, but at the same time limits the control about how the service and data are managed based on the individual needs to the LPA, which may have implications on cybersecurity, e.g. in the way how access control to the service and data is handled.

This quick look at how IT services are usually utilized in LPAs makes one thing obvious: No matter if the service is a citizen or an organizational management service, the most critical asset of LPAs are the data managed and processed by those services. The protection of the data in all stages of the day-to-day processing of the data (including data-in-storage and data-in-transition) needs to be at the core of all cybersecurity considerations. This is, especially in Europe, also very much in line with current legal and regulatory efforts like the GDPR of NIS directive, which apply to local public administrations in the context of data protection and - in many cases - as providers of essential services. To ensure legal compliance, a deep understanding of systems, interactions and processes for the identification, monitoring and mandated reporting of incident and/or breach information is required.

In this sense, a strong cybersecurity requirement in LPAs needs to be a holistic understanding of the IT systems (e.g. server, database, service, network, ...) and the interactions between them in a socio-technical way to understand how the organizational structure can influence the security of e.g. the data that is transmitted, processed and stored by those systems. This includes the identification of the key business processes in day-to-day operations that define the main services provided by an LPA, and how those processes cause data flows and data transformations throughout the systems. The human factor plays a major role in those interactions by managing or administering processes, services or systems, which can have major implications for security. This effort may be a manageable task in small to medium-sized LPAs (number of services, number of users and support personal is limited), but can be a major undertaking in metropolitan areas, where the complexity of the systems may seem overwhelming. Furthermore, the larger the municipality, the more external suppliers that are part of the system play a relevant role in the process.

While the requirement for a holistic understanding of one's systems seems intuitively clear, the reality - especially in larger organizations - follows a more compartmentalized approach. The proper and adequate security mechanisms are put in place on each system level individually (e.g. network, service, application, ...), without a deep understanding of how this affects or relates to dependencies. While most of the times this has no negative impact on the security, it tends to lead to an unnecessarily complex security architecture, and each small change in the system set-up may require a coordinated change in multiple security appliances, like white-listing an IP in a multitude of firewalls if a new client is configured. In general, LPAs usually follow cybersecurity best practices, like applying updates regularly, installing firewalls and anti-virus software and, if applicable intrusion detection/prevention systems (IDS/IPS). Due to limited resources in the public sector, investment in cybersecurity that goes beyond the best practice is often not feasible. For example, procurement of new equipment to replace legacy systems is often not possible due to budget constraints. This can cause security issues if the components are beyond the vendor specified support cycle. Similarly, systematic cybersecurity awareness programs to inform employees about cybersecurity issues and mitigation possibilities are the exception rather than the norm. Awareness usually happens reactive rather than proactive - if an issue happened and is fixed by the IT department, the user will be made aware of the cause (e.g. not to click on suspicious email attachments).

1.5 Cybersecurity awareness in the context of an LPA

We have seen from the previous Sections that LPAs have a specific requirement to protect data, and which common security mechanisms on technical, organizational and legal/regulatory level are available to achieve this task. However, we have also seen that few of the existing cybersecurity measures for organizations take a holistic view on protecting their organizational assets, and that especially the protection of data that traverses many boundaries in day-to-day operation within an LPA may not be covered in current state-of-the-art cybersecurity considerations. In order to address this shortcoming, a new approach of how organizations manage cybersecurity knowledge is required. The key is to achieve a holistic understanding of an organization's cybersecurity status at each level in the organization: collaborative organizational cybersecurity awareness.

To achieve this goal, two major aspects need to be addressed:

1) Cybersecurity needs to be seen as a collaborative effort within the organization, and each department/employee - not only the IT department - needs to feel the responsibility and have the skills to address cybersecurity according to their role in the organization. This necessitates that a certain level of awareness and training about cybersecurity threats and how they relate to the organizational context is available in each relevant department, and that a certain level of collaboration between stakeholders within the organization, as well as with external expert communities (e.g. CERTs/CSIRTs) is possible.

2) The ability to monitor and assess the security state of key assets within the organization in order to be able to detect cybersecurity issues and attacks in real-time, and have the ability to assess and react in a proactive way. Dynamic and data-driven risk and incident management is a way to achieve situational awareness within an organization, and the continuing advancement of artificial intelligence (AI) to detect abnormal behaviour in large data sets is a key enabling technology in this context.

Both of these goals within an organization are supported by the current shift in the cybersecurity landscape – especially in Europe: Driven by the European cybersecurity strategy of 2013 (with the NIS and GDPR being examples for legislation stemming from the strategy), a cybersecurity environment that centres around cooperation and collaboration among key actors in cybersecurity (Network and Information Security actors, Law Enforcement Agencies, Defence, Industry and Academia) is implemented with the aim to gather and analyse cybersecurity intelligence in the respective areas of responsibility, and share this intelligence among the communities and the public. In the context of network and information security, the NIS obliges organizations that are providers of essential services to share information about cyber incidents with the relevant authorities, and the GDPR obliges all businesses handling personal data to share information about any data breach.

A core question is how this does relate to the organizational context and the goals described above? The threat intelligence created and shared by relevant cybersecurity communities based on collaborative knowledge can be utilized by organizations in order to better understand the current cybersecurity landscape. This can range from a better awareness of long-standing and recurring issues and threats, like the statistical analysis of top threats and their mitigation mechanisms, to highly dynamic threat intelligence, like the constant identification of servers and IP addresses used by malicious actors to be able to apply mitigations to such issues in near

real-time. This information can be used to facilitate the collaborative cybersecurity efforts and awareness within the organization, by utilizing context specific information shared by cybersecurity communities within the relevant departments and by the employees for better awareness and preparedness. On the other hand, the legal requirement to share cybersecurity information in case of incidents requires organizations to better understand the cybersecurity implications within their own systems, what damage an attack can cause and what data sources within the systems (e.g. log data on various system levels) can be utilized to detect incidents and, in the worst case, allows forensic analysis of the damage caused by an attack to be shared with the authorities. This in turn raises the level of cybersecurity knowledge within the organization, and creates a basis for more advanced technological systems to build on this understanding and apply automated solutions for better awareness and to ensure legal compliance.

In order to make use of this potential, future cybersecurity efforts for organizations like LPAs need to focus on building supporting technology for the data driven processes described above. This includes a better utilization of the data sources (both those that are able to describe the security state of organizational systems, and those that describe the global cybersecurity state), using AI technologies to automatically detect suspicious behaviour indicated by organizational data sources, identify and correlate it with information provided by competent authorities, and create awareness for the appropriate departments and employees within the organization by distributing the information about incidents and potential prevention/ mitigation strategies in a way that is appropriate to the profiles of the individual employees.

At the same time, the individual socio-technical set-up of each organization, and its implications for cybersecurity, need to be better understood and utilized by AI based cybersecurity systems. The digital footprint of an organization is not only left by its IT components, it is created by the people that interact with the systems and the business processes they conduct utilizing the IT. While a good AI system works extremely well to identify abnormal behaviour in data sources, and has the ability to learn and adapt over time - especially if large data sets are available, the daily routine of an organization often does not follow strict and deterministic behaviour patterns - causing false positive detection of abnormal behaviour. Especially in the context of learning cybersecurity related behaviour patterns, there is much potential in combining specific organizational knowledge to help AI algorithms to better understand individual behaviour and improve detection accuracy. This goes in line with the organizational need for collaborative cybersecurity, and the need to better understand its assets, dependencies and their relevance for cybersecurity described above. This knowledge can be harnessed as an input for training AI algorithms.

Building on the increased organizational cybersecurity awareness that collaboration in the organization and the ability to monitor cybersecurity in an automated way are providing, a baseline security concept is established that can be an enabling factor for more advanced cybersecurity features. In this work we will have a look at two such features building on cybersecurity awareness, namely system self-healing and cybersecurity information sharing.

System self-healing is a concept that allows to prevent or mitigate cyber incidents in an automated way, by for example changing system configuration or applying patches to vulnerable software in case continuous monitoring has detected an issue. In order for this to work, an organization needs to have on the one hand an excellent understanding of its own

systems and dependencies to be able to identify where configuration changes would mitigate or prevent specific cyber threats or attacks. On the other hand, it necessitates the availability of threat intelligence that provides analysis about specific attacks and discusses potential mitigations, which allows AI systems to derive appropriate automated mitigations to be applied to individual systems. Both of those conditions are fulfilled by the cybersecurity awareness concept outlined above, utilizing the threat intelligence provided by cybersecurity communities.

Cybersecurity information sharing describes the concept of sharing information of attacks or applied mitigations with the larger community. The advantage of sharing information in this context is that a community of experts can assess cyber threats or attacks based on data from many individual organizations, and derive better mitigations from this information. For example, European legislation like NIS and GDPR legally require sharing of information relating to cyber incidents under certain conditions. The main problem in this context is to be able to identify all the information that adequately forensically describes specific cyber incidents, ideally based on actual log data. An awareness system as outlined above, based on the understanding of systems and dependencies, allows to automatically identify the main information sources and extract relevant data to be shared with cybersecurity communities or authorities, which can be used to automate the compiling and submission of incident reports.

1.6 Summary and Outlook

In this Chapter we have provided an overview of the current cybersecurity landscape and developments, and which mechanisms are available on the technological, organizational and national/European/global levels to address cybersecurity problems. One of the major concerns in this respect is that cybersecurity is an extremely dynamic problem domain, which has since the early days of the global information network been a race between cybercriminals and cybersecurity experts to devise more advanced cyber-attacks and cyber defence mechanisms respectively. New legal and regulatory efforts especially in Europe acknowledge and account for this reality by taking a collaborative approach towards cybersecurity to be able to identify and react to new cyber threats and cyber-attacks more quickly in order to limit the potential impacts.

We have mapped those developments to the specific environment of LPAs, and we have seen the requirements in cybersecurity to focus heavily on protecting the data managed and processed by LPAs, including citizen and employee data with strong privacy protection requirements. The main identified concern in this regard is the lack of awareness in organizations of how data flows through and is processed by the organizational system during day-to-day operations, and what the associated implications for cybersecurity are in this context.

We have demonstrated the need for gaining awareness through a holistic understanding of the organization and its implications for cybersecurity which can only be achieved through collaboration within the organization. Furthermore, we have pointed out the need for continuous and data driven monitoring of the security state for proactive and timely cyber incident management.

In the following Chapters of this book we will provide more insights into how the CS-AWARE project has created a cybersecurity awareness system that fills the gap identified in this Chapter in the LPA context. Chapter 2 introduces a socio-technical system and dependency analysis (SDA) methodology we applied during the project to increase the ability of LPAs to create awareness and collaborate on identifying cybersecurity relevant aspects, and which allows to identify organizational assets, dependencies, business processes, information flows and relevant monitoring points and monitoring patterns. Chapter 3 describes the technology stack that was implemented during the project to address to address the gap of being able to provide continuous and data driven monitoring of the security state. The system is able to process information from various sources (monitoring points identified in the SDA, and threat intelligence provided by cybersecurity communities like CERTs/CSIRTs) and correlate this information in order to detect incidents and visualize relevant context information and mitigation strategies to the user. Advanced features like self-healing and information sharing are part of this technology stack.

In Chapter 4, the Municipalities of Rome and Larissa who have been pilot partners in CS-AWARE detail their perspective of how CS-AWARE has helped to increase their cybersecurity awareness and collaboration in their organization. Chapter 5 discusses the challenges and opportunities of commercializing such a system in the European LPA marked. Finally, Chapter 6 discusses the importance of awareness and collaboration for future cybersecurity challenges, and the preparedness of the CS-AWARE approach for creating cybersecurity awareness in emerging and future technologies related to the LPA sector.

References

(COMPACT 2018) L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano and L. Sgaglione, "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project," 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, 2018, pp. 573-578, https://doi.org/10.1109/WAINA.2018.00147

(GDPR 2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); http://data.europa.eu/eli/reg/2016/679/oj

(ENISA 2019) The ENISA Threat Landscape (ETL); https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

(EU CS 2013) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf

(Hybrid CoE 2017) The initiative to establish Hybrid CoE originated from the Joint Communication by the European Commission and the High Representative to the European

Parliament and the Council "Joint framework on countering hybrid threats – a European Union response", decided in Brussels on 6 April 2016. https://www.hybridcoe.fi/what-is-hybridcoe/

(IOCTA 2011-2019) INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

(Lamba 2017) Lamba, Anil and Singh, Satinderjeet and Singh, Balvinder and Dutta, Natasha and Muni, Sivakumar Sai Rela, Analyzing and Fixing Cyber Security Threats for Supply Chain Management (2017). International Journal For Technological Research In Engineering Volume 4, Issue 5, January-2017, Available at SSRN: https://ssrn.com/abstract=3492687 or http://dx.doi.org/10.2139/ssrn.3492687

(NIS 2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, http://data.europa.eu/eli/dir/2016/1148/oj

(RUAG 2016) Technical Report about the Malware used in the Cyberespionage against RUAG; GovCERT.ch, 23rd May 2016, TLP: WHITE; https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html

(WannaCry 2017) S. Hsiao and D. Kao, "The static analysis of WannaCry ransomware," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 153-158, doi: 10.23919/ICACT.2018.8323680.

(CC1 2017) Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5, https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

(CC2 2017) Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, April 2017, Version 3.1, Revision 5, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

(CC3 2017) Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

(EUCC 2020) European Union Agency for Cybersecurity, CYBERSECURITY CERTIFICATION: EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS. V1.0 | 01/07/2020, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/

2 The Socio-Technical Approach to Cybersecurity Awareness

Chris Wills

2.1 Introduction

In this Chapter we introduce how CS-AWARE implements one of its fundamental principles; the supposition that an effective cybersecurity management in an organization – including the technology that supports the cybersecurity management - requires a holistic awareness and understanding of the socio-technical system set-up that influences the cybersecurity of the organization, and the interactions between those systems. We show how this awareness can be reached through collaboration within the organization, and how we can utilize the gained holistic understanding as a basis for the technological part of the CS-AWARE cybersecurity awareness solution.

In order best to understand the approach taken in the CS-AWARE project to the systems dependency analysis (SDA) in the two pilot cities and the subsequent design of each pilot city's CS-AWARE system, it's necessary to have some insight into the socio-technical approach that was adopted and applied in the project. This socio-technical approach was used in a holistic analysis of both an organisation's cybersecurity, and of its information systems architecture. In Section 2 we first introduce the concept of socio-technical thinking in general and more concrete approaches for soft systems analysis, like the soft systems methodology (SSM) by Peter Checkland that was utilized in the CS-WARE project. Section 3 describes how the approach was adapted for the CS-AWARE project to achieve the desired level of awareness and collaboration within the organization, and to achieve the desired depth of analysis required to serve as input for the CS-AWARE awareness monitoring technology, including a practical step-by-step guide of how to conduct the analysis workshop sessions. Section 4 concludes the chapter and discusses the results.

2.2 Introducing the concept of socio-technical systems

The term "Socio-technical System" has its roots in Systems Theory. Systems Theory and Systems Thinking are simply a way of looking at some part of the world, by choosing to regard it as a system, using a framework of perspectives to understand its complexity and to undertake some process of change. The key concepts are holism - looking at things as a whole and not as isolated components and systemic - treating things as systems, using systems ideas and adopting a systems perspective.

The term "System" describes an organised entity that incorporates and connects all its components (be they biological, mechanical, digital or human). When operating correctly, a system processes inputs and generates an expected output in a predictable manner.

As depicted in Figure 2.1, systems can be divided into two broad types; "hard" systems and "soft" systems. Hard systems and hard systems thinking, is founded on mathematically-based systems analysis and systems engineering. It assumes that the world is comprised of systems that we can describe accurately and that these systems can be understood through rational analysis. It is based on the assumption that it is possible to identify a "technically optimal" engineering solution for any system. It assumes that we can then write software to create the

"solution".

Hard systems thinking, assumes that there is a clear consensus as to the nature of the problem that is to be solved. However, it is unable to depict, understand, or make provisions for, unquantifiable variables, such as people, culture, politics and aesthetics. It also assumes that those commissioning the system have the ability and power to implement the system.

The hard systems design approach is very good for engineering physical or systems structures that require little or no continuing inputs from people, such as the design and construction of a suspension bridge, or automated process control in an oil refinery, or for control systems for robots used in manufacturing processes, etc. However, for the reasons we have set out above, the hard systems approach cannot analyse, depict, describe or design systems that rely upon inputs from, or interactions with, people.

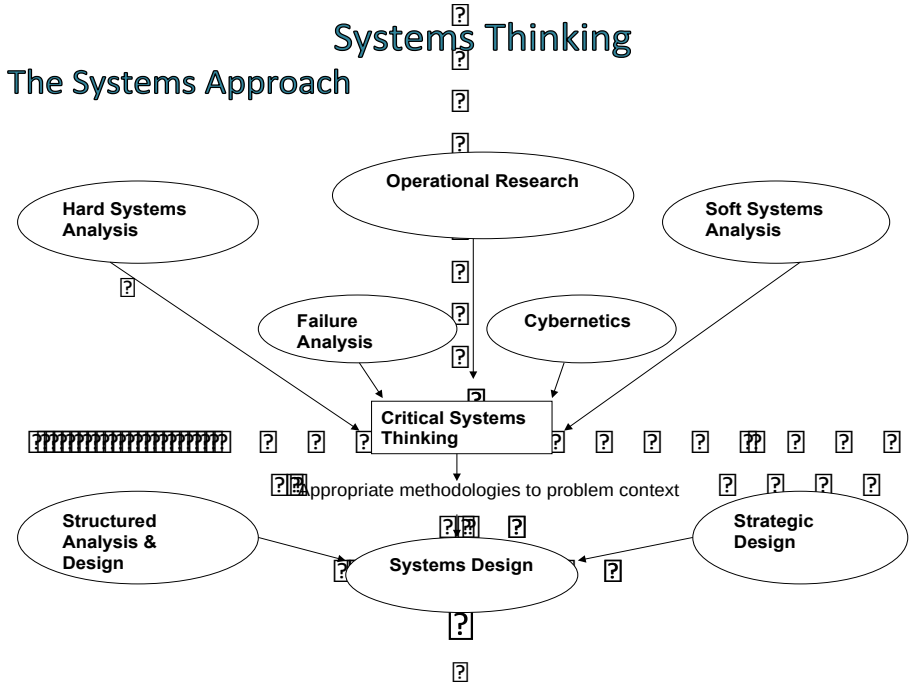

Figure 2.1: Systems Thinking – The Systems Approach

Systems that require human interaction are often referred to as "human activity systems" or "socio-technical systems". Socio-technical systems are those systems whose operations, processes and outputs require some sort of sophisticated and continuing human intervention and interaction in order for the system to work. Any system that requires the input, manipulation or interpretation of data or information by a human is, by definition, a socio-technical system.

2.2.1 Socio-Technical Systems and Soft Systems Design

The dawning of our understanding of Socio-Technical Systems (STS) is usually cited as emerging from the work of Eric Trist and Ken Bamforth (Trist 1951). Their study examined the mechanization of coal mining. The introduction of mechanization in some British mines had led to a lower than expected increase in the amount of coal being mined. Prior to mechanization, the miners worked in three shifts with each shift containing a multidisciplinary team of men with a combined skill-set which enabled them to overcome difficulties encountered in mining the coal during their shift. The first shift cut the coal, the second loaded it for transport to the surface, the third moved the equipment forward to the new coal-face in preparation for the first shift to return and cut the coal. However, each shift contained men with specialist skills which combined and covered all aspects of mining.

When mechanization was introduced, these multidisciplinary teams were disbanded and replaced with teams specialised and skilled only in the particular function of their shift – cutting, clearing away, resetting the machinery at the face. When a shift encountered a problem that was outside their specialism, they had to wait for the return of the shift that contained the appropriate skill-set, who were then able to find a solution to the problem at hand, so that mining could then recommence.

In short, the new system had been designed in such a way as to optimise the mechanization of the coal mining system. However, the human dimension of the process had been overlooked. What Trist and Bamforth's study proved was that systems that relied upon human intervention were far greater than the sum of their mechanical/ technological parts. They could only be properly understood by reference to both their technical and human components. They were not simply "technological" systems, but "human activity" systems; they were "socio-technical systems" because they were sum of both their human (socio) and technological parts. The design of such systems therefore needs to encompass and address both the social and the technological components, hence the term "Socio-Technical Design" coined by Enid Mumford (Mumford 2003). Building on the work of Trist and Bamforth, Mumford developed what she called Socio-Technical Design. In her approach, both the technical and social requirements and components of a system were equally important. Neither the technical, nor the social components of a "human activity system", should be optimised to the point of detriment to either.

Mumford and Henshall (Mumford 1983) argued that, *"The training given to systems analysts is, to say the least, very much biased towards computer systems design, data manipulation and organisation techniques. It recognises the human element of the system in an almost apologetic and certainly mechanistic fashion…. This is not to say that systems analysts do not think about the human factor; they do, but they do not have the methods, tools and training at their disposal which would allow them to design systems that satisfy both the technical system and the social system requisites."*

The authors' are of the opinion that it is still too often the case that "human factors" though not ignored, are not fully and adequately addressed in the design of many current IT and cybersecurity systems.

Mumford (Mumford 1983) identifies three levels of involvement, or user participation. They are, in ascending order of the extent of user involvement in the design process; consensus

participation, where all the users affected by the system are included in membership of the design group; representative participation, where only representatives of the affected users are part of the design team; and consultative participation, where the users or their representatives are consulted at various stages of the design process, but not closely involved in participating in the design of the system.

The extent to which the users can participate in the design process is determined to some extent by the willingness of the host organisation to devolve the responsibility for design. To a greater extent, it is determined by the number of users affected by the system. It is more difficult to extend direct (consensus) participation in the design process to a large group of users than it is to a small group.

Direct participation by a large group in unwieldy and impractical, the logistics involved in a large group of people meeting regularly in a decision making forum are complex and costly. Representative participation in the design of the system is also potentially problematic, for much the same reasons that representative political democracy can be problematic. Consultative participation may not be participative enough to involve the users to the point where they will feel that they own both the process, and the system that results from it. While it is clear that although the participative approach to design is not without problems it is also clear however, even at the consultative level, it still engenders a feeling of ownership of the system amongst the users.

Engendering a feeling of ownership is important. Participation by users in the process of change results in them feeling less threatened by change. A reduced perception of threat is likely to reduce the users resistance to change. As important, is the deep-rooted emotional feeling of ownership all of us experience when we embody our intellect and creativity in the creation of something external to us. Users who feel that they have a personal stake in the system will be highly supportive of it.

The other outcome of user participation is that the knowledge elicitation process is made much more effective: *"Firstly, it is a fact that the people with the greatest knowledge of the existing formal work system, and the people with the most knowledge of the informal system, are the people who are responsible for their operation. They therefore have the greatest potential to successfully design a system which overcomes the present systems shortcomings"* (Mumford 1983, pp.120).

Notwithstanding these practical justifications for using an STS approach for the design of information systems, there is also a moral philosophical dimension to the argument. People should be involved in the design of the systems with which they work. They should work in situations where they rewarded equally well in both intrinsic and extrinsic terms.

Mumford's STS methodology as depicted in Figure 2.2, ETHICS (Effective Technical and Human Implementation of Computer-based systems), has fourteen stages, the core method involves the following:

- Forming the design group, be it on a consensual, representative, or consultative basis.
- Appointing an "expert" analyst designer, who is attached to the group, to act in the role of "facilitator", helping the group reach conclusions about what is feasible, by offering expert advice, rather than by directing the group to a particular conclusion.

- The design group then identifies the primary social and technical requirements of the future system. The group creates a list of social alternatives, and a list of technical alternatives, which will contribute to attaining the primary social and technical objectives. These two lists will contain those features that should be embodied in the future system, in rank order of desirability.
- Social alternatives will focus on those features that provide the best social solution to the problem, (typically, those features which improve the quality of working life of those who will work with the system, or are affected in some way by it). These features will be considered in terms of what is possible **(social possibilities)**, what is desirable **(social needs),** and what is undesirable or prohibitive **(social constraints)**.
- Technical alternatives will be concerned with those features which will provide the greatest technical improvement to the problem, and as with social alternatives, will be considered in terms of what is possible **(technical possibilities)**, what is desirable or prohibitive **(technical needs)** and **(technical constraints)**.
- Comparisons are then made between the social and technical alternatives, and a list containing those social and technical alternatives, which are not mutually exclusive, is compiled.
- These potentially **available solutions** are now evaluated in terms of costs/benefits, and the extent to which they satisfy both the primary social and technical objectives, the outcome of this process being the highest-ranking STS solution.

Latterly, Mumford's work has been used as a base for other STS approaches (HUSAT 1988), and latterly has been incorporated with other approaches into a flexible methodology called Multiview (Wood-Harper 1985), detailed discussion of which is beyond the scope of this chapter. Moreover, Mumford's participative approach is also reflected in current "AGILE" development methods.

The approach taken in the CS-AWARE workshops (in the pilot cities) largely follows Mumford's lead in terms of the design group, which in both of the pilot cities, involved the participation of the greatest possible number of stakeholders, both in the SSM and the story telling workshops.

Cybersecurity is a socio-technical problem because it is utterly and absolutely reliant upon the knowledge, appropriate behaviour and timely intervention of personnel, in order for data and information security to be maintained. Therefore, cybersecurity systems are usually (although not exclusively), socio-technical systems and as such are best designed using a socio-technical design approach.

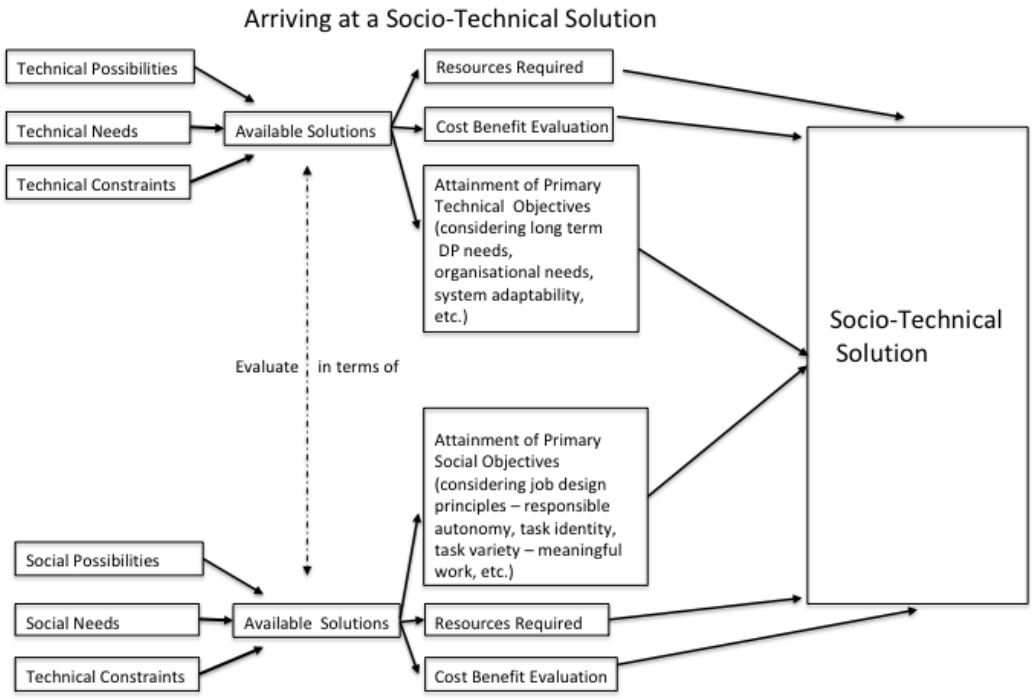

Figure 2.2: Arriving at a socio-technical solution using the ETHICS methodology (Mumford 1968)

2.2.2 Soft Systems Methodology

For the CS-AWARE project we have utilized the Soft Systems Methodology (SSM), an approach that builds upon the socio-technical approach and soft systems design to analyse existing and organically grown complex systems. The approach emerged from the work of Peter Checkland and his colleagues. Checkland (Checkland 1981) observed that systems involving people - "Soft Systems" are often very complicated, fuzzy, messy, ill-defined and are typified by unclear situations, differing viewpoints and unclear objectives, which include politics, emotion and social drama. This is the type of system domain for which Checkland's Soft Systems Design approach, is highly appropriate and to which it should be applied. This is of course the case with the analysis and design of a cybersecurity awareness system such as was the focus of the CS-AWARE project.

The idea underpinning SSM is that of creating a comparison between what can be seen in the

real world and what can be examined using systems thinking, as depicted in Figure 2.3.

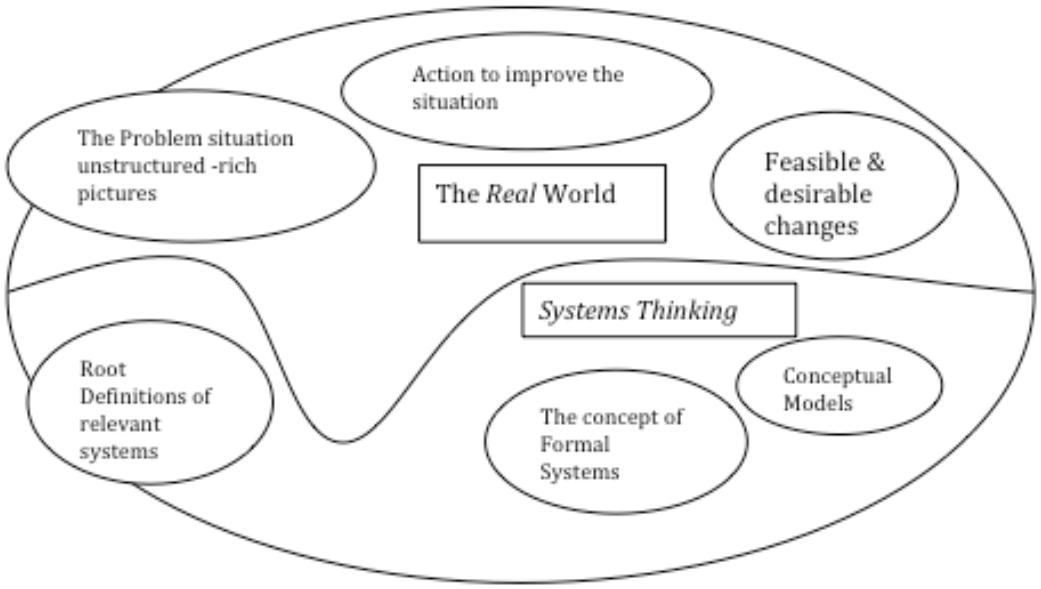

Figure 2.3: SSM core concepts

Checkland's Soft Systems Methodology has seven steps, as seen in Figure 2.4, which form the approach. Although the methodology involves seven stages, it may not be necessary to apply all seven to a given problem situation. In some cases, interventions that significantly improve the problem domain become extant in the earlier stages of the method. The fist stage is that of exploring and thinking about the problem situation that is under consideration. As is set out above "Human Activity Systems" are often messy and ill-defined, contain sometimes few, if any measurable objectives and consist of differing views coloured by organisational politics typified by high social drama. The second stage involves creating "Rich Pictures" (RP's).

RP's are a representation of the problem domain. They utilize "cartoon-style" techniques to portray a complex situation and concentrate on:

- Structure - Key individuals, organisations etc.
- Process - What could be or is happening
- Climate - Pressures, attitudes, cultures, threats etc.

There are no formal rules that need to be applied when drawing RP's. Contributors to a picture are free to use any graphical or linguistic approach they choose to use in their picture(s).

RP's are a tool for understanding a problem situation whether it's a system or not. They are a mixture of drawings, pictures, symbols and text. They represent a particular situation or issue and they are created from viewpoint(s) of the person or people who drew them. They can both record and evoke insight into a situation. RP's are pictorial 'summaries' of a situation, embracing both the physical, conceptual and emotional aspects of a problem situation. There are no rules that apply to the drawing of rich pictures. There is no right or wrong way to

construct an RP, it is entirely in the hands of the person, or the group of people, who are drawing the picture. No artistic skill is required!

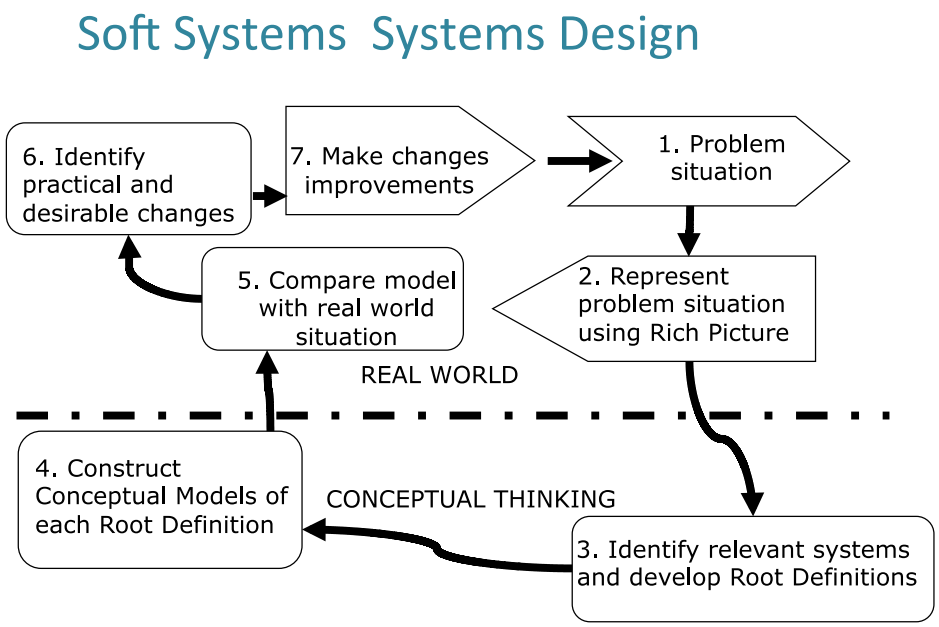

Figure 2.4: The seven steps of the SSM methodology

The process of creating a RP is simple. The stakeholders taking part in the SDA, construct a diagrammatic representation of the problem domain. This RP depicts both the physical (logical) and the political social and cultural elements that they have identified in the problem situation that is being examined. The full participation of stakeholders at this stage of the method is essential, as they will have a far deeper understanding of the problem situation than will an external analyst or consultant. The RP attempts to capture and represent both the physical infrastructure and the processes, but also the relationships between the stakeholders. These are represented in the RP's in order to gain an understanding and appreciation of the problem situation. The Rich Pictures should contain 'hard' information and factual data, as well as 'soft' information; subjective interpretations of situations, including aspects of conflict, emotions etc. The RP should give a holistic impression which can then be further analysed, refined and understood by the subsequent stages of the SSM methodology. RP's are powerful; they enable those drawing the pictures to express their understanding of a problem domain or a system in great detail.

As an example, the RP in Figure 2.5 depicts the respective check-in operations of two mythical competing airlines, Pacific Air and Atlantic Air. This RP is machine drawn for the sake of clarity, RP's are usually hand drawn.

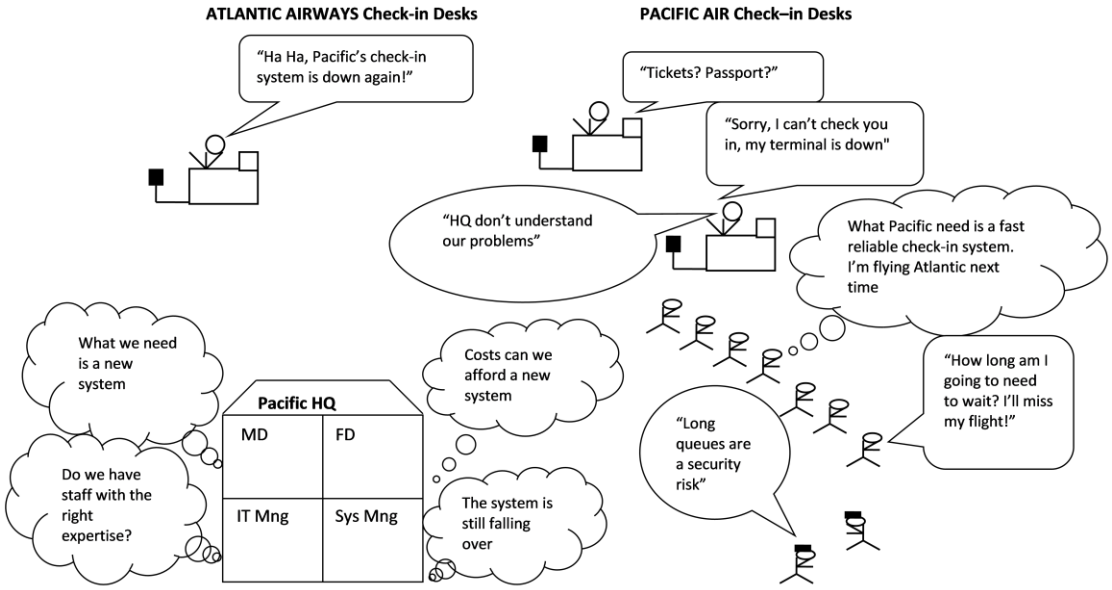

Figure 2.5: Example of a Rich Picture

Pacific Air has a problem with their passenger check-in system. The check-in clerk's terminal keeps malfunctioning and the clerk cannot check-in the passengers and their luggage. The customers are understandably disgruntled, as are the check-in staff. Pacific Air's management have a variety of views from the managing director understanding that they need a new system, the financial director is worried about where money will come from to pay for a new system, the IT manager is worried about whether they have the right staff with the right expertise and is concerned that that's perhaps why the system keeps failing. The airport management are concerned about the security risk that the long queues at check-in creates, as none of the passengers have passed through security at that point. Atlantic Air meanwhile is delighted, because they hope to pick up more passengers as a result of Pacific Air's failure.

Once the Rich Picture has been constructed, in third stage, relevant sub-systems are identified and defined using "Root Definitions". A Root Definition is not an attempt to describe some real, existing 'system'. It is an attempt to learn about a complex situation to enable changes to be made which encapsulate the essence of these systems, the 'whats' (what does it do?) rather than the 'hows' (how does it do it?). The Root Definitions describe the core transformation activities and processes of the system – the conversion of inputs into outputs. A Root Definition of the RP above would be:

"An airline owned passenger check-in system that enables passengers to check in their baggage and enables airline staff to issue passengers with boarding cards in a manner that is consistent with the safe and timely operation of the airline's departure schedules".

Checkland used a mnemonic - "CATWOE" to check that all of the necessary components of a problem situation were represented in any a RP of that situation so as to ensure that the 'Root Definitions are complete and accurately represent the problem situation portrayed in the Rich Picture.

Customers	Those who benefit in some form from the system
Actors	The people involved
Transformation	The development of outputs from inputs
Weltanschauung	The 'world view' a holistic overview of both the transformation processes and the problem situation
Owner	The person(s) with control
Environmental constraints	Physical boundaries, political, economic, ethical or legal issues

A "CATWOE" of the airline RP would be as follows:

Customers	The passengers
Actors	The airline staff
Transformation	Unchecked baggage become checked, passenger tickets supplemented with boarding cards
Weltanschauung	The efficacious effective and efficient operation of the Airport and the Airline (it works with minimum waste and meets the expectations of the passengers, the airline and the airport)
Owner	The Airline
Environmental constraint	Time, safety, security effectiveness (passengers and baggage departing to the same correct destination)

The fourth stage of the method is that of creating conceptual models. Once the Root Definition(s) have been constructed and have been compared with the Rich Picture and checked against CATWOE, Conceptual Models can be constructed. The Conceptual Models are formed from the actions stated or implied in the Root Definition(s). Of course, each Rich Picture may be interpreted from quite differing 'world view points' Conceptual Models be derived from a Root Definition even though knowledge of any 'real-world' version of the activity is lacking.

A Conceptual Model is like an activity sequence diagram, but is aimed at representing a conceptual system as defined by the logic of the Root Definition and not just a set of activities. It is **not** a representation of what exists in reality, nor is it necessarily a representation of what ought to exist. It should contain only those actions that would have to be carried out, and the order in which they would have to be carried out, if the system in the Root Definition were to

function. Conceptual models will differ depending on the of the view-point of the observer. The view-points and understanding of the airline RP by the check-in staff, the Financial Director and the IT Director, are all quite different.

Having developed a top level, primary activity Conceptual Model as the one illustrated in Figure 2.6, each of the activities identified are modelled in a second level Conceptual Model like the one shown in Figure 2.7, once again based on our airline problem situation.

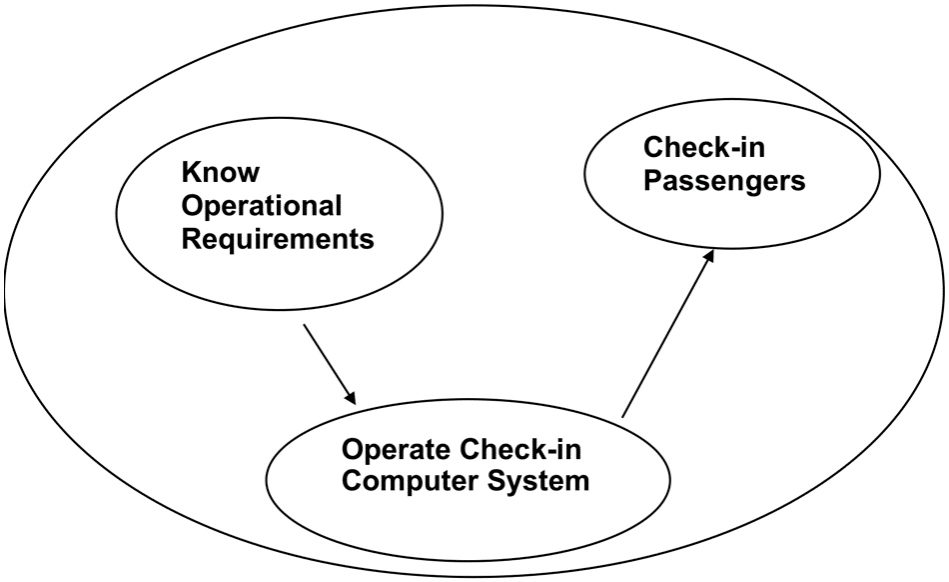

Figure 2.6: A Top-level Conceptual Model of the Check-in Process

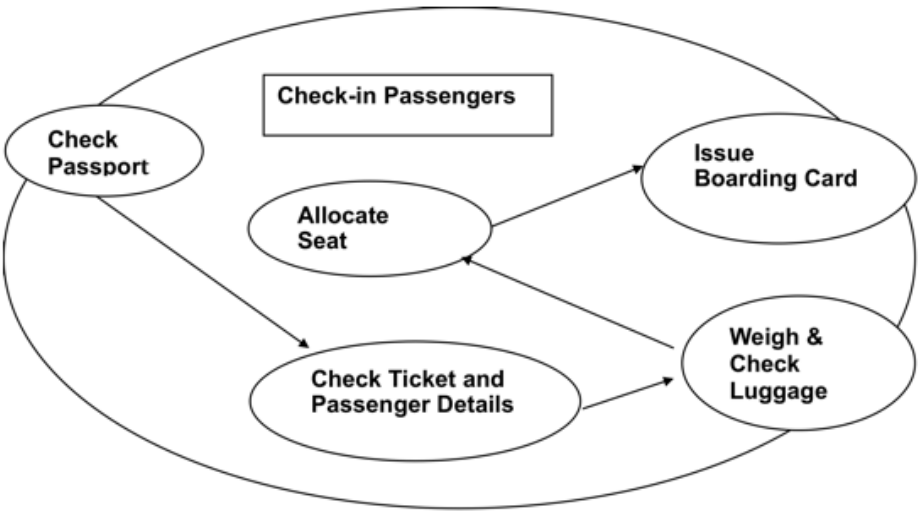

Figure 2.7: A Second Level, Secondary Activity Conceptual Model

In the fifth stage the Conceptual Model(s) are checked against both the Root Definition(s) and the Rich Picture. A good way of performing these checks is to ask three questions: Do the activities exist? Who does them? Why do it that way? The analyst(s) need to imagine that the Conceptual Model is actually operating in the real world. They can identify a real process from the Rich Picture, follow its sequence in the Conceptual Model and compare how the sequence would operate in reality. This process can be represented using a chart:

Activity in Conceptual Model	**Present in Real World Situation (Rich Picture)**	**Comments**	**Include on Agenda**
Check Passport	Yes	Process tasks place independent of check-in computer system	No
Check passenger and ticket details	Yes	Dependent upon operation of check-in computer system	Yes
Weight and check luggage	Yes	Process tasks place independent of check-in computer system	No
Issue boarding card	Yes	Dependent upon operation of check-in computer system	Yes
Allocate seat	Yes	Dependent upon operation of check-in computer system	Yes

The sixth stage of the methodology is that of identifying practical interventions (changes) that can be introduced into the problem domain to improve the current situation. Usually the interventions that are required are obvious and emerge as a result of drilling down through successive layers of conceptual models. Sooner or later, practical and practicable interventions (changes) that will improve the problem situation become apparent. There may be several interventions that can be made. These may be social, technical organisational or economic in nature. In the preceding example of Pacific Air's check-in system, is it the case that system too old, and has become obsolete and difficult to maintain, as the MD suspects? Perhaps the skill set of the technical staff needs to be improved, as the IT manager believes? Perhaps some coding errors have somehow been introduced into the booking system software? Using SSM to drill down through all of these socio-technical aspects of the problem domain will reveal the issues and the appropriate and practicable solutions represented by the methodologies seventh and final stage.

2.3 SSM in action: The CS-AWARE approach

The systems dependency analysis (SDA) that formed the core of the project was based on SSM as described above. The idea being that the users of an organization's systems use SSM to help them express and give an account of, their (often tacit), knowledge in dedicated workshops. These workshops included participants from all levels of the organization (e.g. managers, technicians, administrators and end-users).

The goal of the SDA is to be able to interface an organization's system to the CS-AWARE technical solution for continuous cybersecurity monitoring and awareness. For this purpose, three main aspects need to be derived:

- **Assets, dependencies and monitoring points:** Identify critical assets, the dependencies between those assets and potential monitoring points (log files) to surveil those assets.
- **Business processes and information flows**: Identify critical business processes for the organization's day-to-day operations, and the information flows that those processes produce through the organization's systems (assets and dependencies).
- **Observable parameters and system behaviour:** Identify how the system behaviour (and the boundaries between normal/abnormal behaviour) is reflected within the monitoring points (log files) and identify observable parameters in those files that capture this behaviour.

The following Sections will describe the procedure that was followed to conduct the analysis workshops as a step-by-step guideline. This guideline was originally published in CS-AWARE deliverable D2.5 "Guidelines and procedures for system and dependency analysis in the context of local public administrations". The deliverable should be consulted for further detail and context, for example concerning suggestions for how to organize SSM workshops in an organization.

2.3.1 A practical guide to the CS-AWARE analysis approach

This Section describes in detail the 3 stages of SSM analysis conducted in the project. The first stage is concerned with structural analysis of assets and dependencies, the second stage is concerned with analysis of business processes and information flows, and the third stage is concerned with behavioural analysis and identification of monitoring patterns.

2.3.1.1 Structural analysis – Understanding the socio-technical system in terms of assets and dependencies

The context of this stage of the analysis is to gain a holistic picture of the critical assets and their dependencies within an organization that are relevant for cybersecurity monitoring and awareness. These include (but are not limited to), the perspective of the user that interacts with those systems, the manager that oversees the systems operations, and the admins/technicians that ensure day-to-day operation of the systems. The concrete set-up of each organization will be highly dependent on organization, but following procedure should guide through a successful workshop:

1. Start the workshop by giving a general overview of the context and purpose and the expected outcomes and results of the workshop. All participants should have received this guide before for pre-workshop preparation, but a general introductory session will ensure a common understanding. Reserve time for comments and questions.
2. Ask the workshop participants to identify the most critical assets and/or assets related to the most critical business processes of the organization. While those will be highly dependent on the organizational context, a good starting point are assets related to:
    a. Financial systems of the organization
    b. Systems that relate to data that is managed by the organization, for both public sector and commercial organizations
    c. Systems that relate to services provided to a large customer base (citizen services in the public sector, commercial products in the private sector)

    Depending on the size of the group, divide the workshop into groups no larger than five for providing an initial list of critical assets. The groups should prepare their results in form of a rich picture and present it to the workshop participants. It is to be expected that the input and discussions in the larger group will provide additional viewpoints that substantiate the initial results. If necessary, repeat this step by shuffling the group participants until a consensus among the participants about the most critical assets is found.
3. At the next stage, the goal is to concentrate on the initial list of critical assets, and identify all the relevant elements and dependencies that are required by those assets to operate, from the interactions on the end user side, to the technical elements that process and store data. While the concrete set-up highly depends on the organizational set-up, experience has shown the elements required to ensure service operation are usually part of:
    a. the network infrastructure,
    b. the application service infrastructure,
    c. databases and
    d. security appliances
4. Participants should work in groups no larger than five to create a high-level picture of their understanding of the organization's assets, dependencies and interactions between the two. Groups should be formed that are expected to contain perspectives from different organizational levels. For large and complex organizational set-ups, it may be necessary in the first round, for the groups to work on different aspects or the systems (e.g. network, services, security, …). For low to medium complexity set-ups, each group can aim to develop a holistic understanding in the early phases.
5. The results of the group discussion should be put to a rich picture on a flip chart, after which each group should present the results of their discussion to the other groups. At this stage it is to be expected that a lively discussion among the workshop participants will take place. This will reveal the tacit knowledge and differing viewpoints of participants, and will facilitate the development of a holistic understanding of the system. After this exercise, the groups should be asked to develop and refine their understanding, and provide a more detailed overview, including the input from the first round of discussions. If necessary, re-order the groups based on outcomes of first round. Results should again produce a rich picture, which is presented to the analysts and other participants. This step should be repeated until a consensus among the workshop participants on the holistic understanding of the organizations systems and dependencies is agreed.

6. As a last step for information collection related to the first stage of system and dependency analysis, potential monitoring points, data sources (log files) that allow continuous monitoring of previously specified assets, need to be identified. As in previous steps, it is to be expected that those sources will relate to elements on the network, service, database and security appliance level. Based on the previously achieved common understanding, it may be possible to discuss this aspect in the large group. However, it may be necessary to follow a similar process as before and divide the workshop into groups, each depicting the results on rich pictures and presenting the results of each group to all of the workshop participants.

Once a consensus on the holistic understanding of the organizations asset and dependency set-up has been achieved and potential monitoring points are identified, the first stage of system and dependency analysis is concluded. It is important that, once the workshop results analysed, an additional workshop session including all participants is required to double-check the graph and amend missing information. This can be done in preparation for stage 2 of the workshop, or in the context of the first workshop session of stage 2.

2.3.1.2 Business process and information flow analysis

While the objective of the first stage of the analysis is to understand the system in terms of assets and dependencies, the goal of this stage is to identify how day-to-day operations map to the asset and dependency graph in terms of information flows caused by relevant business processes. Following procedure should guide through a successful workshop:

1. Start by reviewing the system/dependency graph from the first stage. If this has not been done in between the workshops, reserve time for reviewing the system and dependency graph and allow for modifications until a consensus is reached among the participants.
2. Based on the critical systems/services identified in the first stage, give the participants some time to define business processes that are required to conduct day-to-day operations within those services. If deemed necessary, the participants can be asked to prepare for this task before the workshop. Depending on the number of participants, groups may be formed, with each group focusing on one of the identified critical systems/services. Make sure that multiple organizational viewpoints are present in each group.
3. The resulting list of business processes should be visualized in the form of a rich picture, and each group should present their results to the workshop participants. It is to be expected that the understanding of business processes will be complemented by the input/discussions within the group. If necessary, additional rounds of group work, followed by presentations of results should be conducted until a consensus is reached. Groups may be shuffled if necessary.
4. Once a consensus is reached, the workshop can move on to define the business processes in detail. Experience has shown that the CATWOE method described in Section 2.2 is an excellent approach to analyse business processes.
5. For each process identified, a CATWOE list should be produced. Depending on group size and number of processes to analyse, this can be either done with all workshop participants present, or in group work. The results should be presented as a rich picture and presented to the group. The process should be repeated until a consensus is reached for each business process CATWOE list.

6. As a result of the CATWOE analysis, the identification of the actors and data transformations, provides sufficient information to map the business process to the asset and dependency graph, by identifying the information flows resulting from the processes identified through the organizations systems. For each process, identify which assets are involved in conducting the process, from end-user interaction, to communication over network and from data processing by the back-end service to data storage. It may turn out that relevant assets were previously omitted, which should be complemented accordingly.
7. A review of potential monitoring sources (log files) to observe system behaviour should be conducted, and it should be identified if additional monitoring sources come to light in the context of business process observation.
   Once a consensus regarding the information flows per business process has been achieved, the second step of SDA analysis is concluded. After the information flows are modelled within the CS-AWARE asset and dependency graph, they should be discussed with the workshop participants. This can be done in preparation for, or during the workshop sessions of the third stage.

2.3.1.3 System behaviour analysis

Having derived structural information in stage 1 and process information in stage 2, the only missing aspect to interface an organization's system to CS-AWARE for continuous cybersecurity monitoring is the definition of behaviour that day-to-day operations relating to the identified business processes, and how this behaviour is reflected in the monitoring points (log files) identified in steps 1 and 2. Moreover, the boundaries that determine normal and abnormal behaviour as recorded by various parameters logged within the log files, are the basis for the definition of monitoring patterns by CS-AWARE experts. In general, there are two main pattern types relevant for CS-AWARE: (1) behaviour-based monitoring patterns that monitor behavioural patterns in order to detect abnormal and potentially malicious behaviour, and (2) indicator-based monitoring patterns that associate uniquely identifiable security information (vulnerability, virus, network intrusion, …) in order to associate context for awareness.

Mapping abstract behaviour to concrete and, in most cases, deep technical information found in log files is a more involved process than in the two previous phases - especially for workshop participants that do not usually think in technical terms. Experience has shown however that with careful preparation and by following the process laid-out in this guide, the contributions from workshop participants will lead to significant results with regards to identifying abnormal or suspicious system behaviour and to how this behaviour is reflected in log data. For this to be successful, careful preparation by the analysts before the workshop is required: A sample of all log files used as monitoring sources, as identified in stages 1 and 2, should be investigated and all the logged parameters within those files should be identified. Monitoring sources are of course highly dependent on the organizational set-up and will require individual analysis. A few generalizations can be given regarding the expected data on the database, the service, the network and the security appliance level. Both databases and application services usually keep audit logs for data operations and authentication, which are highly relevant for behaviour monitoring. The network and firewall security appliance logs usually contain various aspects relating to network traffic, and are both relevant for behaviour and indicator-based monitoring. Antivirus and IDS/IPS security appliances logs detected events and are usually relevant for

indicator-based monitoring. Once pre-workshop preparation is completed, the following procedure should guide participants through a successful workshop:

1. When the workshop starts, a quick recap of the results of the first stage (system and dependency graph) and second stage (business processes/information flows) should be presented. Allow for time to capture additional input from workshop participants for corrections/ additions that have come to light since the previous workshop sessions. If necessary, repeat relevant analysis elements from stages 1 and 2.
2. The previously identified monitoring points (log files) should be introduced. Based on the pre-workshop preparation, a general overview of the log file structure and the available parameters should be given. Together with the participants, the meaning of each parameter in the specific context of the organization and relevant business process should be defined in discussion until a consensus is found. While many parameters have a clear purpose and meaning, there may be parameters that are context specific and require input from the organizational context to be fully understood.
3. The review of the log files establishes a common understanding of the log file contents, and the information about system behaviour that is captured by each parameter. The next step is to ask workshop participants to define behaviour and/or scenarios that
    a. Are considered disruptive or malicious to the various business processes reflected in the data
    b. Are something that the organization (represented by the roles of managers, technicians, service users, …) want to be made aware of
    c. Are something that is not part of the current monitoring activities and/or something that cannot easily be monitored within the current set-up

    Depending on the group size, the workshop can be divided into groups, while making sure that different organizational perspectives are present in each group. The results of the group discussions should be presented to all workshop participants, discussing and substantiating the scenarios by input from other group members. Those scenarios that are deemed relevant by the consensus of the group, are to be further investigated in the next steps. Unrealistic or irrelevant scenarios should be discarded by consensus. This exercise may be repeated, shuffling the group participants, until no more relevant scenarios can be identified.
4. Identify parameters in the log files that are able to capture behaviour of the scenarios defined in the previous step and how this behaviour would be reflected in the data logged by those parameters. For behaviour/scenarios, it is expected that the most relevant log files will be on the database and service level.
5. For each identified behaviour reflected in one or multiple parameters, the boundaries between normal and abnormal behaviour are to be defined by consensus of the workshop participants. For example, if a behaviour/scenario to be monitored is the access time to a specific service (logged by the authentication log), the normal behaviour may be expected as login during business hours (e.g. 9:00 to 17:00). However, the tacit knowledge of workshop participants may reveal there are users that work late, which would extend the normal operating hours (e.g. 9:00 to 20:00). Repeat above steps until all identified scenarios have been discussed and a consent was found for parameters that capture the specific behaviours and their boundaries between normal and abnormal.

6. Especially the log sources that are mainly relevant for indicator-based monitoring (e.g. security appliance logs) may not be involved in any of the discussed behavioural scenarios. While they may not require input from the workshop participants in order to derive unique event identifiers that can be utilized by CS-AWARE for providing additional context, they should still be discussed during the workshop sessions, since participants may have additional tacit knowledge about the organizational context of the log sources that may help to derive more relevant monitoring patterns.

2.3.2 Examples from the CS-AWARE pilot use cases

Several workshops conforming to the procedures described in the previous sections were run in each of the pilot cities. At the start of the series of workshops in both of the cities, an overview was given of the Soft Systems Methodology. The participants in each workshop were asked to draw a RP of the mission-critical systems in their respective cities. As we have previously set out, and as we discuss further below, we defined mission-critical systems as being those systems which contained or processed either sensitive personal information (such as would fall under the provisions of the GDPR), or information or processes which were vital for the city's ability to provide vital services to it's citizens. This would include systems and processes that were used to maintain and handle the city's finances.

Figure 2.8, Figure 2.9 and Figure 2.10 show examples of such a "top level" RP's in Larissa and Rome and an associated description of the applications, systems and networks represented in each of the RP's.

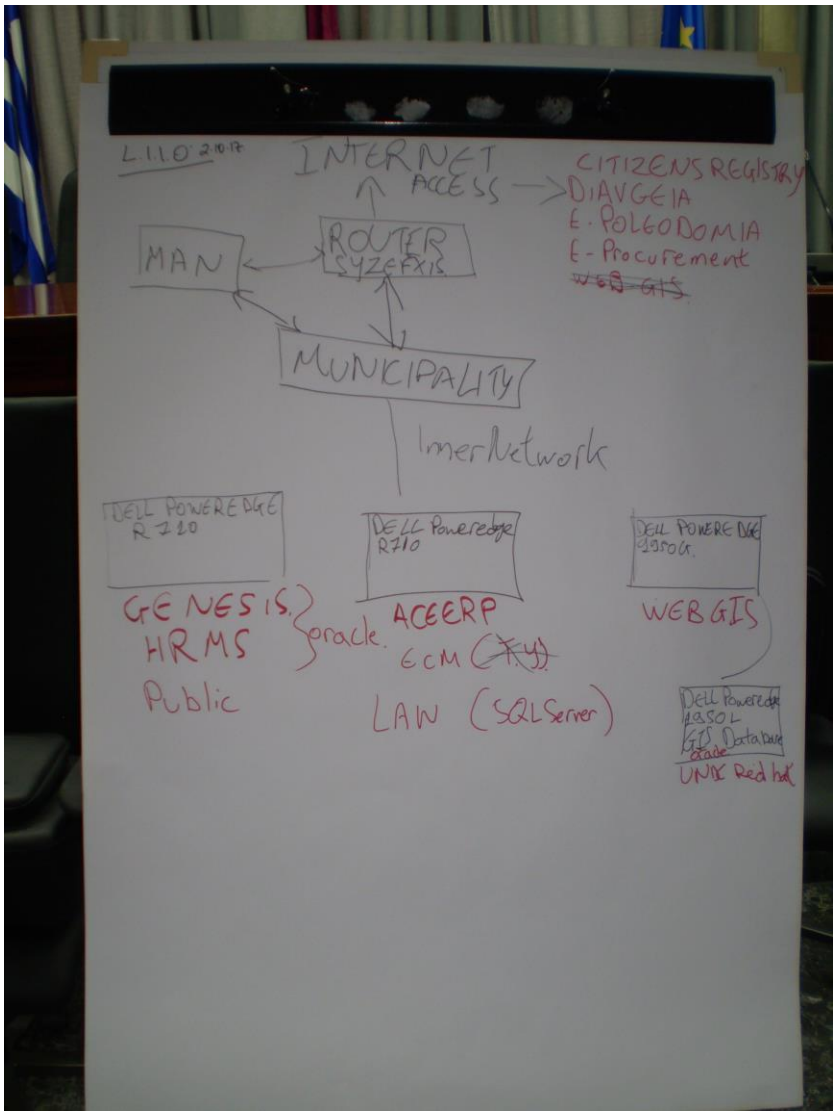

Figure 2.8: Top Level RP Larissa

Larissa RP 1 above gives an overview of the city's network and main services. The only gateway from the City's systems to the Internet and telephony to the outside world is via a router called SYZEFXIS. The SYZEFXIS router is run by the Greek Government and is a nationally provided system. The Cities of Larissa, Elassona and Kileler all use the SYZEFXIS router.

SYZEFXIS is connected to both the Metropolitan Area Network (MAN) and to the three servers located in the Town Hall. The R710 host Genesis, (the City's ERP system that is used to manage income and expenditure) Genesis handles information about both suppliers and citizens and tax and debt collection. The system is used for maintaining the civil registry, for records of document signing and for the cash desk.

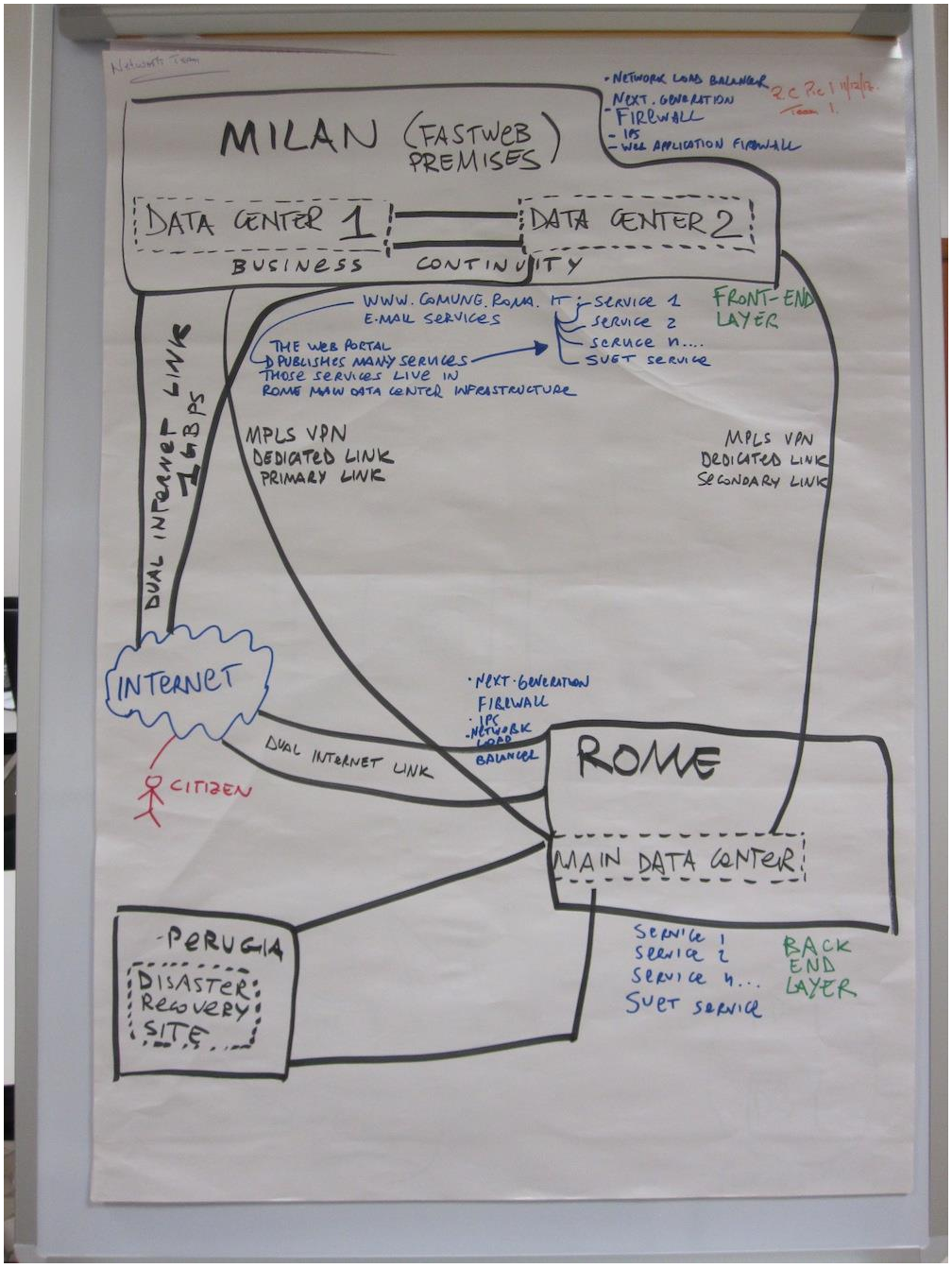

Figure 2.9: Top Level RP1 Rome

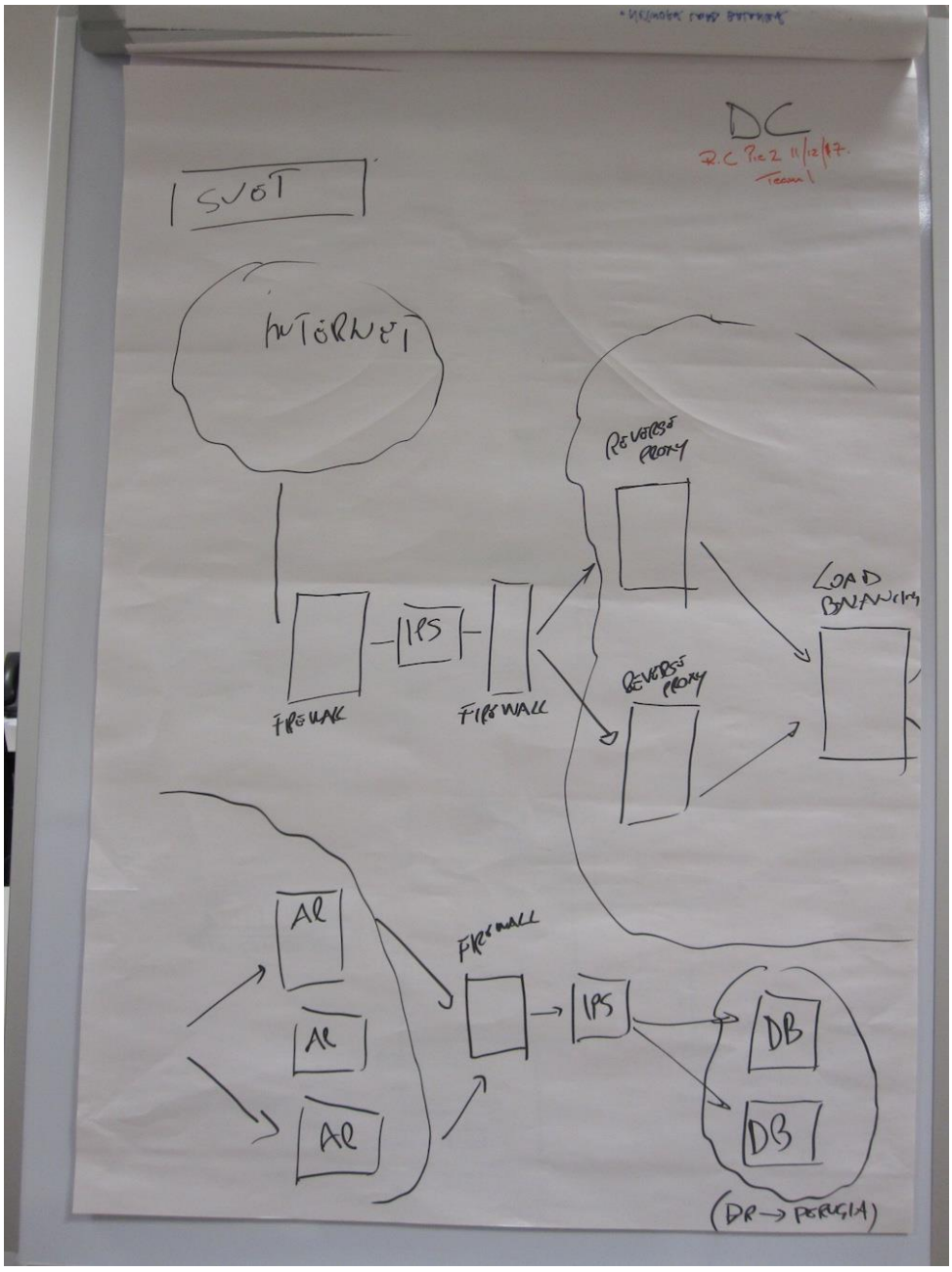

Figure 2.10: Top Level RP2 Rome

The two top level RP's for Rome are above. Rome's data is held outside the city. In Milan there are two data centres in two different locations in the city of Milan working an active-active cluster according to Business Continuity architecture. Data centres in Milan are owned by Fastweb (a supplier), that also provides Roma Capitale with Internet and network perimeter security services. Fastweb has its own disaster recovery site in Rome to ensure RTO and RPO needed by Roma Capitale.

Roma Capitale's main Data Centre is located in Rome and it's duplicated in Perugia for disaster recovery purposes.

The site in Rome is connected with the main site Milan with two dedicated MPLS (multi protocol label switching) VPN links (1Gbps each link): this network connection is geographically differentiated (each link has its own bidirectional path from Rome to Milan) to enhance reliability, service availability and network resilience.

The Roma Capitale portal (www.comune.roma.it) is on a server located in Milan; while other services (including SUET service) is located in Rome. Front end user access (common citizen) to Milan site; while an employee directly access to Rome infrastructure.

The mail server and related protection services are located in Milan site.

Security is enforced and monitored in by following elements:

- DDOS Mitigation services to protect Rome Capitale portal email services;
- Web application firewall to protect Rome portal;
- Network load balancer;
- Next generation firewall, both in Milan to protect Roma Capitale portal and email services (network perimeter security) and in Rome to protect each and every web service published by Rome Capitale portal homepage (Data Centre security) Many firewall layers exist.
- IPS, both in Milan and Rome basically deployed following next generation firewall architecture described above.

The above top-level RP's were the starting point for the dependency analysis in both of the pilot cities. Each of the systems represented in each of these RP's were then the subject of further examination and analysis. Each were themselves the subject of a further Rich picture, with each new RP drilling down through the functionality and connectivity of each application, system and network until all of those participating in the workshops were content that they had accurately captured, described and understood the functionality, connectivity and dependency of all of the applications, systems and networks. In a manner analogous to creating "Root Definitions", the workshop participants then wrote descriptions of their top-level RP's. CATWOE was then used to check the completeness of the RP's. An Example of a "CATWOE" appears below in Figure 2.11.

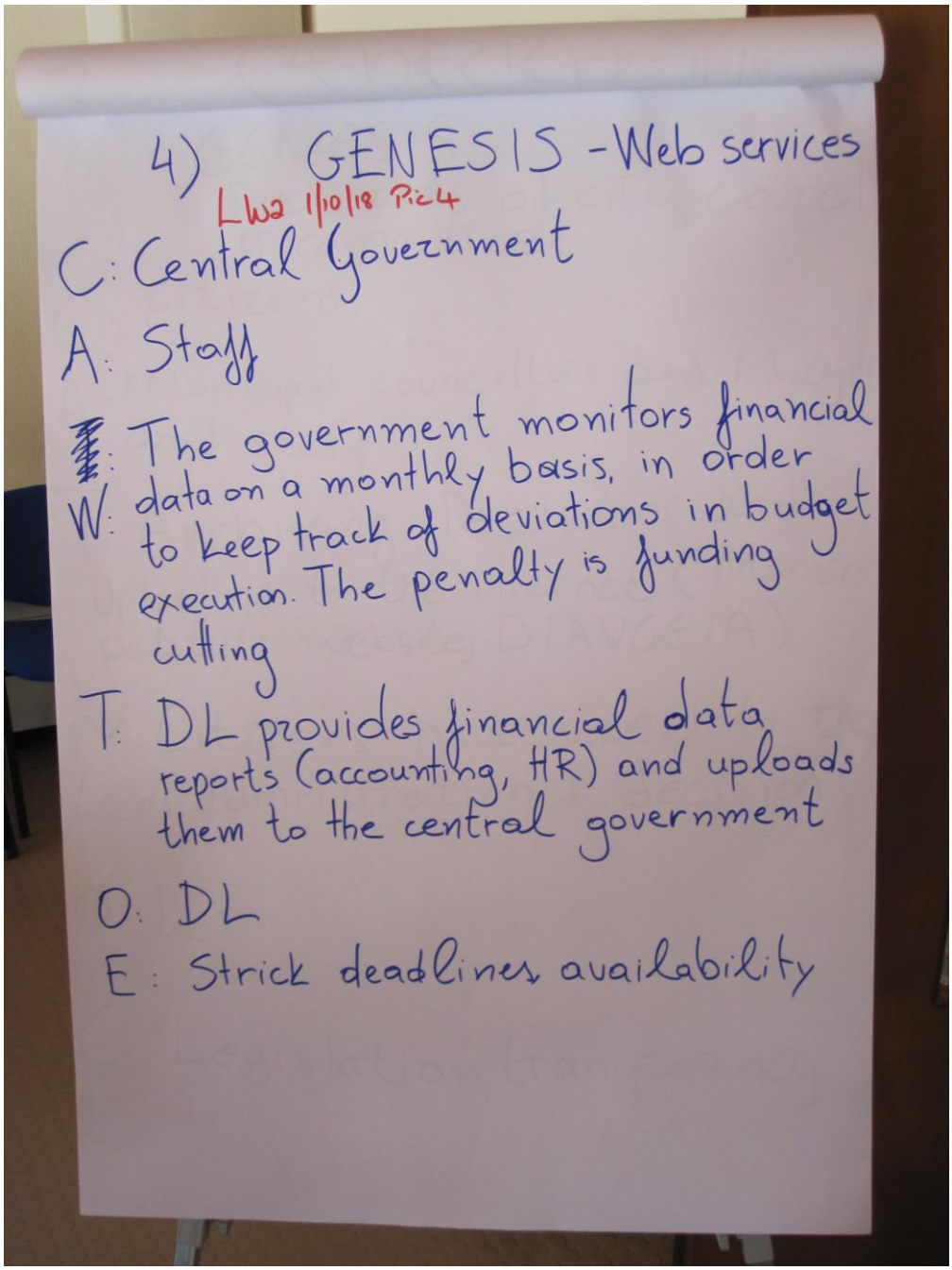

Figure 2.11: Example of a "CATWOE"

The key aspect of the CATWOE in terms of the SDA is that of the "Transformation(s)" identified in the RP. The transformation(s) are a description of the systems and networks that have been captured in the RP. These descriptions are the key to unlocking an understanding of how an organisation's networks and systems work and helps to enable the identification of key critical systems and the critical business processes that are conducted on those systems.

Key critical systems are either:

i) Those systems that are vital to the financial well-being of the organization.
ii) Those system which collect, process or transmit sensitive or personal data or information, or via which systems sensitive or personal data or information can be accessed.

In addition to being used to check the completeness of an RP, CATWOE was also used to help identify key features attributes, capabilities and vulnerabilities of a system, as is done in the context of the CS-AWARE SDA analysis.

Once this process was completed and in the following rounds of workshops, machine-drawn representations of the applications, systems and networks were created and further refined and checked for completeness by the workshop participants. For example, Figure 2.12 shows an illustration of a dependency graph created by this process. Figure 2.13 highlights the assets of the graph that are involved in the information flows that a specific critical business process of this example organization generates in day-to-day operation.

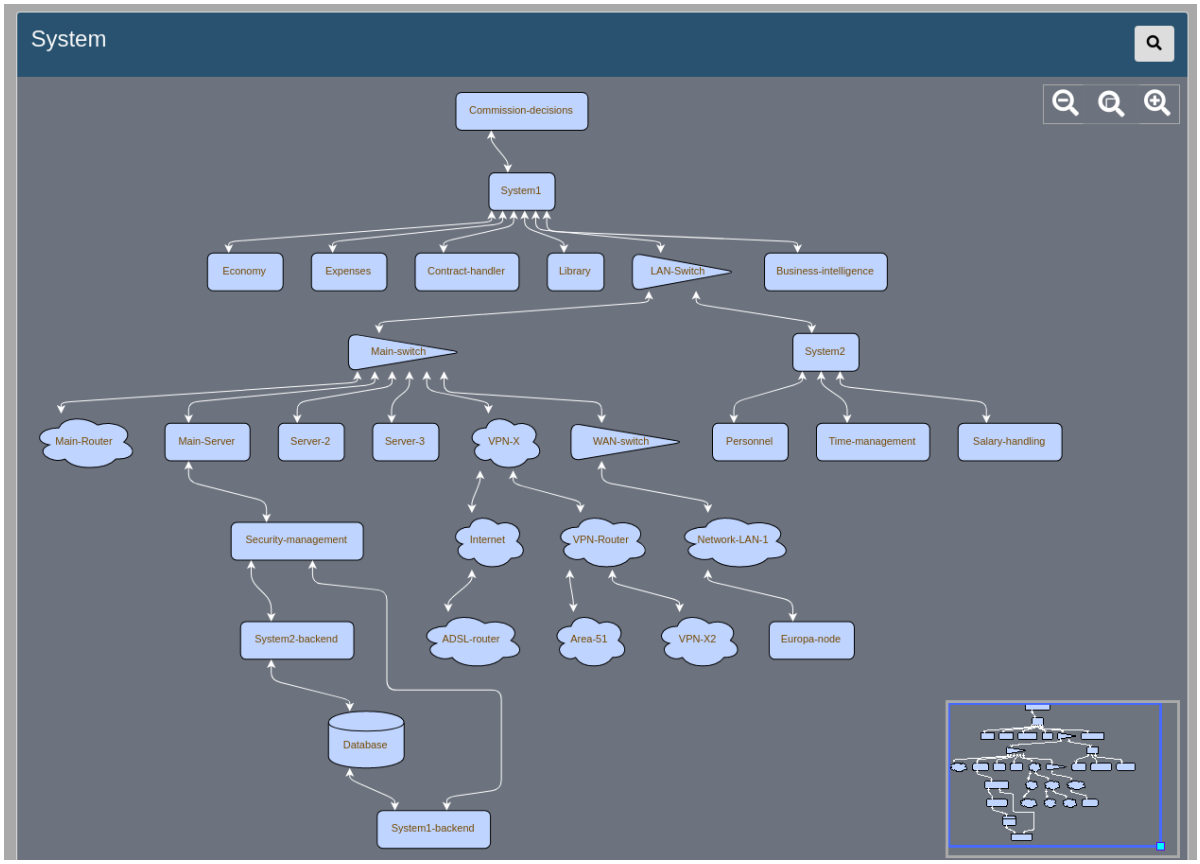

Figure 2.12: CS-AWARE system and dependency graph

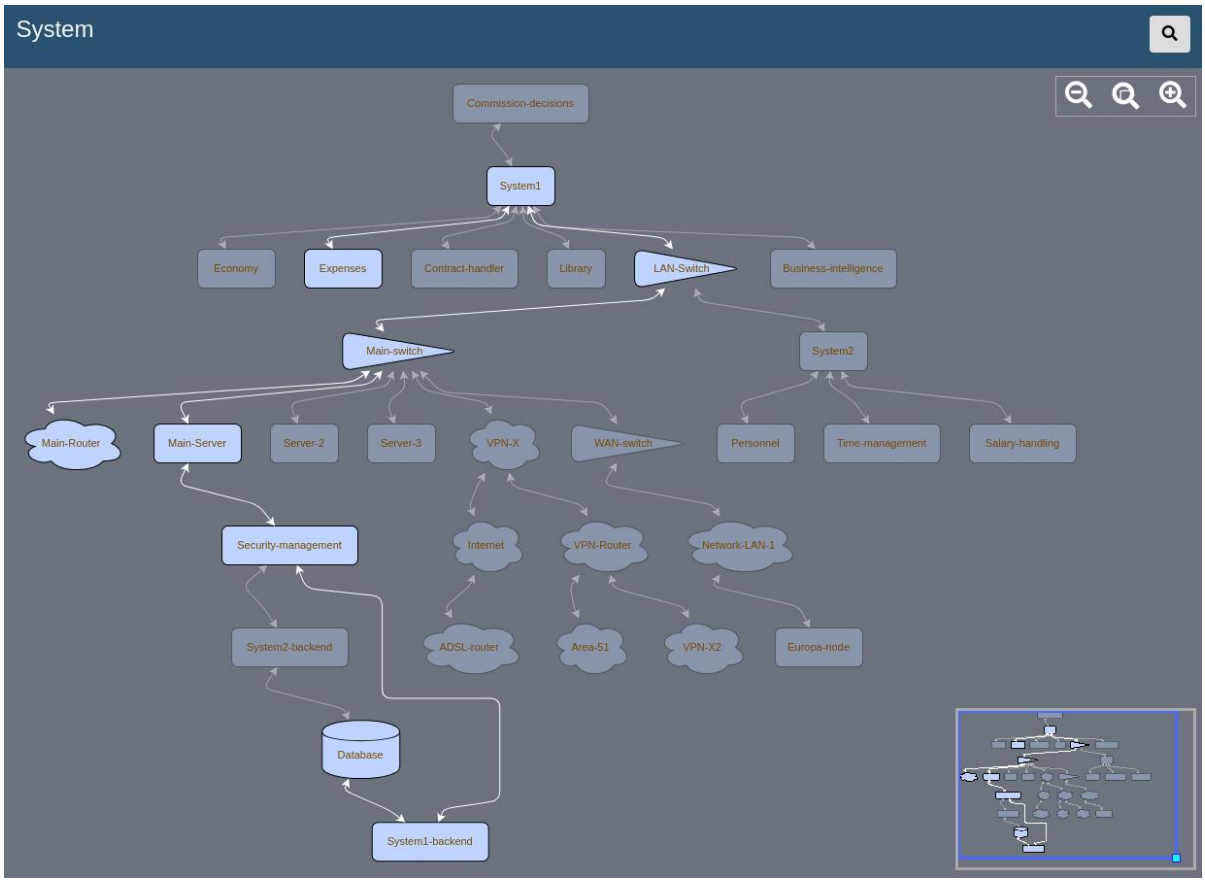

Figure 2.13: Example of a business process information flow

Furthermore, the table below gives an example of an illustrative monitoring pattern to be utilized for real-time monitoring of abnormal behaviour of the database utilized by a critical business process. The relevant monitoring parameters as well as the ranges are developed by the workshop participants from available log files based on the actual situation relevant for the use case.

Pattern name	**Pattern Parameters and ranges**
Suspicious Database Modification Attempt	**Abnormal login time periods**: normal range (5am, 9pm) max range (0am to 12pm) **User type** type: (admin, user) **Number of Users** normal range (0;15000)

	max range (0; 50000) **Login session duration time**: Logoff time - Logon time direction of search higher better **If login rejections number >5 /hour - suspicious** **boolean: true/false**

2.4 Outcomes and Conclusions

Our experiences with adapting and applying the SSM approach for SDA analysis in the LPA cybersecuirty context have been overwhelmingly positive. We have experienced that the value of this type of analysis, and the learning effect that the participants in the LPAs experience, is much greater than the project has originally anticipated. While all the participants in the workshops are experts in their domain and area of expertise, the value of collaboration within the organization to tackle a specific problem domain like cybersecurity from the holistic perspective is something that is not part of the usual activities of LPAs. The value of cooperation becomes more apparent the greater the size and complexity of a municipality is, since the organizational structures become more departmentalized and specialized. As a side effect of the analysis that was not anticipated to this level, municipalities who apply this approach can expect to develop a much more detailed and deeper understanding of their systems, procedures, their cybersecurity vulnerabilities and requirements implicit in their compliance with the GDPR. A more in-depth analysis of the value of SSM analysis will be given in Chapter 4, which represents an account of the CS-AWARE project from the LPA point of view, including considerations for structural and organizational changes to improve cybersecurity awareness based on the CS-AWARE approach and results.

In the context of being able to utilize the SDA results as a configuration basis for the technological cybersecurity awareness monitoring solution, the outcomes of the analysis have fulfilled the requirements in each respect. To reiterate, the main properties for the CS-AWARE solution to be able to LPA cybersecurity monitoring are:

- **An asset and dependency graph:** A structured representation of the asset and dependency analysis result, which can be used as an evolving knowledge repository of each assets cybersecurity context.
- **A model of information flows in the system and dependency graph:** CS-AWARE enables the information flows for each identified critical business process to be modelled within system and dependency graph.
- **Identification of observable parameters and the boundaries between normal and abnormal behaviour:** The definition of CS-AWARE cybersecurity monitoring patterns requires the definition of observable parameters, as well as the boundaries between normal and abnormal behaviour observed at the identified monitoring points (log files).

We were able to gather and model this information in a structured format for both CS-AWARE pilot use cases. We were able to show that the significant difference of size and complexity of each use case (a mid-sized and a metropolitan area municipality) had no impact on the ability

to achieve comparable results in both cases. Chapter 3, which details the different aspects of the technical part of the CS-AWARE solution, will show in more detail how this information is utilized to provide cybersecurity awareness.

References

(Trist 1951) E.L. Trist and K.W. Bamforth, "Some Social and Psychological Consequences of the Longwall Method of Coal- Getting." Human Relations, 4:3-38, I951.

(Mumford 2003) Mumford E, Redesigning Human Systems, IGI Publishing, Hershey P.A, & London 2003.ISBN: 1932777888

(Mumford 1983) Mumford, E. & Henshall, D. (1983) "Designing Participatively" Manchester Business School, Manchester

(Mumford 1968) Cf. Mumford, The Economic Evaluation of Computer Systems Vol. 3 National Computing Centre Ltd. 1968

(HUSAT 1988) HUSAT Research Centre, Loughborough University (1988) "Human factors guidelines for the design of computer-based systems" Ministry of Defence Procurement Executive/ Dept of Trade & Industry, London

(Wood-Harper 1985) Wood-Harper, A., Antill, L. & Avison, D. (1985) "Information Systems Definition: The Multiview Approach" Blackwell, Oxford

(Checkland 1981) Checkland, P.B. Systems Thinking, Systems Practice, John Wiley & Sons Ltd. 1981, 1998. ISBN 0-471-98606-2

3 The design of CS-AWARE Technology

Alexandros Papanikolaou, Kim Gammelgaard

3.1 Introduction

This Chapter focuses on the technological aspects regarding the implementation of the CS-AWARE solution, which provides system administrators with cybersecurity awareness about the information system they are in charge of, by analysing the information found in the log files of their most critical systems and visualising the results in an appropriate manner. In this way, system administrators are quickly informed whether there are indications of suspicious activity occurring in their systems and they also receive recommendations or suggested actions to take for specific instances of the aforementioned issues. As a result, system administrators do not need to spend time analysing and correlating potential indicators to form an opinion on the cybersecurity status of their systems. They can use this time for further understanding the information and the potential decisions presented to them by the system. Furthermore, by collecting and analysing publicly-available cyberthreat intelligence, the CS-AWARE system is able to deduce whether there are cyberthreats in the wild that could harm a specific information system it monitors and issue the necessary warnings accordingly.

The functionality that CS-AWARE provides aims to help organisations deal efficiently with the cybersecurity challenges their information system is faced with, taking into consideration that they usually lack both the expertise and resources to properly address these issues. The chapter presents the deployment of the CS-AWARE system at two pilot Local Public Administrations (LPAs) of different sizes, as examples of organisations that lack resources to allocate for dealing with their cybersecurity issues. Nevertheless, the solution could easily be applied to SMEs as they share similar characteristics with LPAs as far as their information system and resources (both human and financial) are concerned.

The individual seven components of the CS-AWARE solution are initially presented, explaining their functionality and role in the overall system. Then, the CS-AWARE Framework is presented, exhibiting how the aforementioned building blocks interact among them to achieve the desired system functionality that essentially involves analysing data, deriving cybersecurity awareness and conveying it to the user.

The implementation phase presents the various challenges related to the complexity and heterogeneity of the systems that had to be addressed from a technical perspective, as well as the main key points where decisions had to be made in order for a viable solution to be produced, given that there were developer teams from different companies/institutes involved, with different backgrounds, expertise and work culture. The integration and deployment phase was equally challenging, since all the aforementioned building blocks had to communicate among them and also with the designated information system nodes of each one of the two pilot LPAs (Municipality of Larissa, Greece and Municipality of Rome, Italy).

Finally, the user interface design is presented, demonstrating how it evolved from its initial conception to its final “look and feel”, as well as the functionality and the information it presented to the user. This was the result of several rounds of iterations, where feedback was collected from users, was analysed and incorporated into the user interface through appropriate

modifications. Moreover, the implementation of certain changes in the user interface triggered modifications in the functionality and/or the information provided by the other building blocks, so as to offer the highest possible level of cybersecurity awareness to the user.

3.2 The CS-AWARE system architecture

In this Section the architecture of the CS-AWARE system is presented, starting from the description of the main components it consists of. Then, the presentation of the CS-AWARE framework follows demonstrates the logical grouping of the said components, as well as the information flows among them during their operation.

3.2.1 Description of the main components

Before going into the details of how the CS-AWARE was implemented and the related decisions that had to be made during this course, it is worth presenting in brief the various components and their purpose in the integrated system. The seven modules comprising the CS-AWARE system are as follows:

- System and dependency analysis
- Data collection and storage
- Data analysis
- Multi-lingual semantics support
- Data visualisation
- Cybersecurity information exchange
- Self-healing

3.2.1.1 System and dependency analysis

By applying the Soft Systems Methodology (SSM), the organisation's critical nodes are identified. Then, the System and Dependency Analysis Support Tool is used to create a "system graph", with all the aforementioned nodes, showing the connections and the data flows among them. What is more, each node also includes the necessary information that can be used for uniquely identifying it as a node (e.g. hostname, IP address), as well as with respect to the type and the version of the operating system running on it. This information is made available in structured form (JSON) to any other module that may require it for fulfilling its operation.

3.2.1.2 Data collection and storage

This module involves a data collection framework, able to aggregate and ingest data from four main sources:

1. Logs from servers, databases, applications and network devices from within a Local Public Administration's (LPA) systems.
2. Information about packages and software installed on servers.
3. Cyber threat intelligence from specialised websites and feeds.

4. More general cybersecurity-related notifications and warnings collected from social networks.

All this data is fed into the CS-AWARE system for analysis to detect threats or provide pointers for mitigations. In addition, the data collectors are responsible for performing any data anonymisation that may be required.

3.2.1.3 Data analysis

This is the threat detection engine of the CS-AWARE system, where log data is analysed, correlated and matched against patterns that would identify specific threats and/or suspicious activity. For example, a significantly high number of reads by the same user for a given database may mean that the said user account has been compromised and data is being downloaded/extracted from the database. Provided that the database system has transaction logging enabled, a suitable pattern would be able to detect the aforementioned behaviour.

It is worth emphasising that these patterns can be either generic or organisation-specific. The first category includes more "universal" cases, such as a brute-force attack attempting to guess user passwords. The second category includes cases that are closely related to the organisation's business operations and/or information systems. For example, if its employees are expected to interact with the information system only within a specific time frame (e.g. 09:00-17:00), then a suitably crafted pattern could easily detect any user activity outside the designated time frame.

What is more, certain patterns are provided in a generic form to avoid bearing too much detail. Nevertheless, they still need to be adopted according to the structure and set-up of the organisation's information system, in order to function properly and be effective. For instance, detection of the failed user log-in attempts in a custom software application may require examining specific database tables and columns that have non-generic names.

3.2.1.4 Multi-lingual semantics support

This component essentially consists of two subcomponents, each performing a different function: The NLP Information Extraction component and the Multilanguage Support component.

The former subcomponent attempts to extract any cybersecurity-related information from social network feeds (e.g. Twitter) that could be proved useful for the CS-AWARE threat detection engine. This approach was based on the fact that cybersecurity experts and companies tend to share cybersecurity-related information through social networks (e.g. a new malware kind exploiting specific ports or services), well before notifying the official repositories, such as the Common Vulnerabilities and Exposures repository.

Any alerts and information about cyberthreats that exist in a language other than the system administrator's mother tongue can impose an extra layer of complexity, while trying to deal with them. The latter subcomponent thus aims at translating any kind of text written in a foreign language to the end user's mother tongue.

3.2.1.5 Data visualisation

The data visualisation component is responsible for visualising the threats, the threat level, the possible self-healing strategies and the information shared with the Cybersecurity community. Moreover, it communicates back to the system any user responses related to the

aforementioned functions, as well as lower level administration. Since it is the only system component that conveys cybersecurity awareness to the user, it is presented in more detail in Section 3.3 below.

3.2.1.6 Cybersecurity information exchange

In the cybersecurity field, any information or knowledge about a threat (newly-discovered or not) is very valuable for proactively protecting organisations and for detecting threats more efficiently and effectively. For instance, if the characteristics of a threat discovered in an organisation are made public (e.g. which ports it attacks or uses to propagate, IP addresses it originates from), then another organisation can do the following:

- Proactively block the malicious IP addresses to protect itself from being attacked in the first place.
- Perform a targeted search in its log files to determine whether traces of activity resembling the behaviour of this given threat also exist in their system and, nevertheless, they have not been detected yet by the installed security mechanisms.

The cybersecurity information exchange (CIE) component is responsible for the transmission of cyber-threat intelligence (CTI) to external entities. CTI is made available in a structured form and more specifically according to the STIX 2.x standard, to facilitate interoperability and consumption of the provided information by external entities, such as threat intelligence platforms, Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). Data sanitisation, anonymisation and marking are deployed to secure data privacy and protection of classified information prior to making it available to external parties.

3.2.1.7 Self-healing

Self-Healing aims to assist LPA administrators respond to identified vulnerabilities and high-risk threats by providing customised healing solutions or recommendations. The Self-Healing component is a fully-supervised solution that uses the results of the Data Analysis component and looks for the most appropriate mitigation solution among its self-healing database and those provided by the external sources. The chosen solution, according to the administrator's preferences, will either be applied automatically or request their approval or simply be presented in the form of a recommendation.

3.2.2 The CS-AWARE framework

The various components comprising the CS-AWARE solution were briefly presented in Section 3.1.1. A high-level view of the information flows among these components is presented in Figure 3.1. Furthermore, the components have been divided into three distinct layers:

- The **Data Extraction layer** covers all components responsible for defining relevant data and extracting it, as well as the sources themselves.
- The **Data Transformation layer** summates all components tasked with transforming and analysing the data in some way. The data may be filtered and adapted, if necessary, before being processed by the modules.

- The **Data Provisioning layer** is meant for visualising and sharing the detected incidents and data patterns, as well as for the automated system reactions and recommendations performed by the self-healing module.

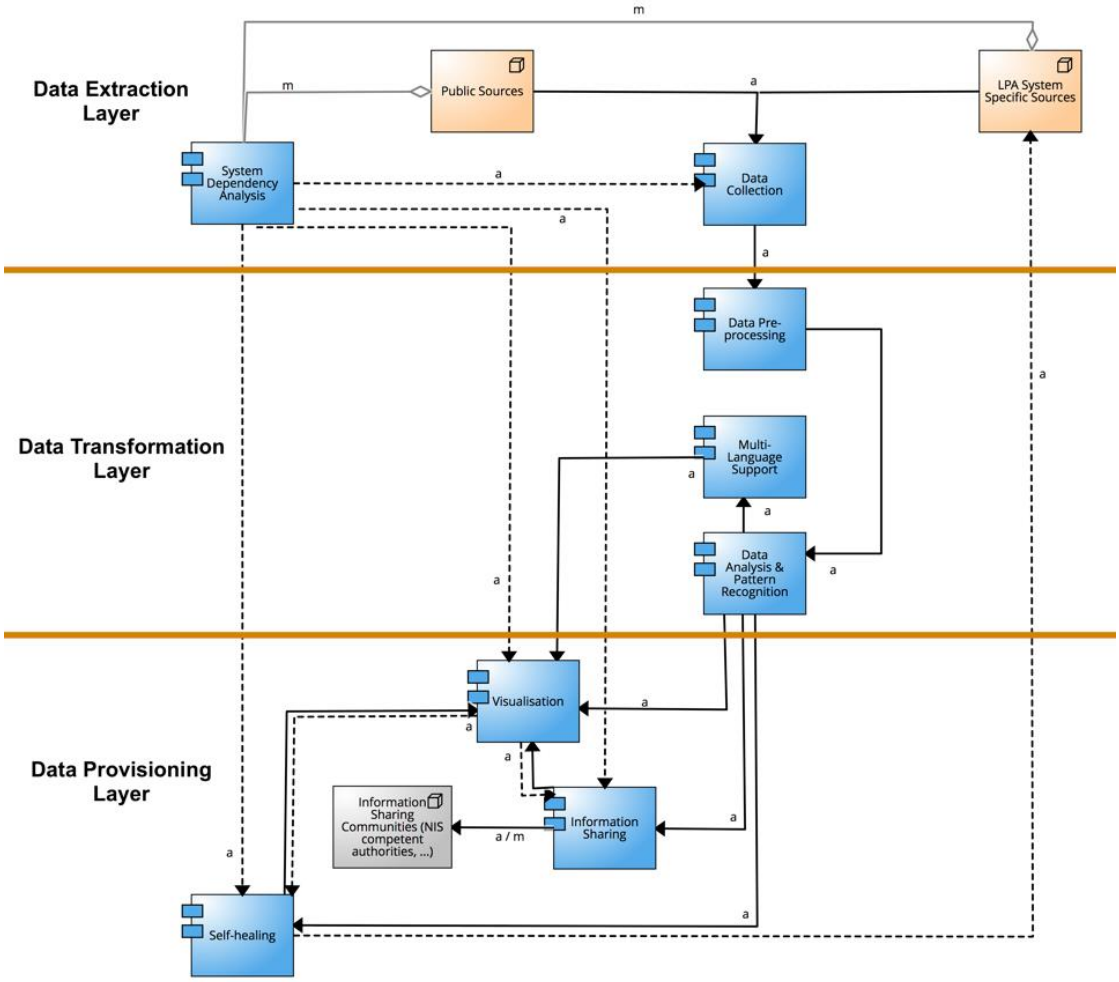

Figure 3.1: Information flows within the CS-AWARE framework.

3.3 Development and integration

The CS-AWARE modules can be divided into two main categories: The ones that were developed from scratch and the ones that were based on already existing components. The latter had to be adopted accordingly, in order to offer the required functionality. In this Section the adaptation of the existing components is presented, followed by the various decisions that had to be made and/or taken during the integration phase, as well as any challenges encountered.

3.3.1 Existing components adaptation

Some of the components comprising the CS-AWARE solution were developed from scratch, whereas others were based on existing technologies that were adopted appropriately, according to the requirements.

The System and Dependency Analysis Support Tool is based on GraphingWiki, an extension of the open-source wiki engine MoinMoin that was developed in 2006 to support the collection and visualisation of data. It was successfully used in software protocol and malware analysis by introducing additional meta link syntax and (other capabilities). The tool was further adopted to meet the needs of CS-AWARE by creating a new interface and new graphical elements for visualising the relationships among the nodes (e.g. double-headed arrows). Its functionality was further extended to support exporting of the contained information in JSON format, to facilitate the automated processing of any modules requiring access to it.

The Data Collection component was based on data collectors that had been developed in the past. For acquiring the logs data, collectors were installed at key points of the LPAs' systems and they feed the CS-AWARE system with the data to be analysed for threats. In order to comply with the GDPR requirements and at the same time keep the complexity low, data anonymisation was decided to be performed at the source, before transmitting it to the CS-AWARE system.

The Data Analysis component is based on MAARS (Multi-Attribute Analysis Ranking System), a proprietary software developed by Peracton that is able to process and analyse any number of parameters, with their unique settings and then filter and rank items very fast. Its adaptation for the purposes of CS-AWARE was mainly the creation of suitable threat patterns. For instance, in order to detect a suspicious database modification attempt, the database audit and access logs need to be processed to detect several parameters, such as the frequency of login attempts per day, login time periods, and IP addresses of unexpected ranges. Each parameter is assigned an appropriate weight according to its importance/severity and the aggregated result denotes whether the criteria for a given threat pattern were satisfied or not.

The NLP Information Extraction subcomponent was based on Graphene, a rule-based information extraction system developed in the context of research conducted at the University of Passau. The main strategy behind Graphene is to simplify complex sentences before applying a set of tailored rules to transform a text into the knowledge graph. During the CS-AWARE project the research prototype evolved into a technology that is both easy to deploy as a service and integrate as a product. A new extraction layer was also added for transforming complex categories into a graph of fine-grained knowledge, to facilitate processing and extraction of conclusions.

3.3.2 Planning the components' integration

CS-AWARE was originally designed to be installed as a cloud-based architecture, using serverless components and other features that are not available in traditional internal datacenter setups. However, during the pilots implementation phase, the original plan had to be changed due to an inflexible requirement of deploying the solution only inside a municipal datacenter (Roma Capitale).

At the same time, development was being performed by separate groups and it therefore became evident that the development process would benefit from using a separate virtualisation/container engine for each component.

The decision to use Docker as the component instance and Docker Compose as the integration framework was taken quite early. The main reason that steered the decision towards this

direction was that this approach had been followed by the University of Vienna in the past and it seemed very promising, as it could deliver both local and cloud-implementations with relatively little effort. This architecture has proven its value so far.

When choosing Docker, it is also possible to use container-orchestration tools like Kubernetes, also part of Docker Enterprise. However, for the purposes of CS-AWARE, it was assessed that it would add more complexity than benefits to the project. Nevertheless, since Docker was being used anyway, it was possible to add the solution's custom setup to existing Docker Enterprise/Kubernetes server farms with relative ease.

When architecting applications like CS-AWARE, scaling is an important factor that needs to be considered. By using Docker it was possible to have a full-scale setup running on a well-equipped laptop. On the one hand, this gave the ability to perform development in a production-like environment. On the other hand, for the actual production environment, it was possible to split the modules onto high performance servers, as well as split database and storage with ease during configuration. In this way, the load could be handled very efficiently and the aforementioned flexibility proved to be very valuable in the development and deployment process.

3.3.3 Integration challenges

Due to the nature of the log data that would be collected for analysis, there were serious privacy issues that had to be dealt with, since, among others, IP addresses and usernames were anticipated to be contained in the municipalities' system logs. Significant effort was put in ensuring that there would be no privacy violations within the scope of the CS-AWARE project. This involved communicating with the competent Authorities of Greece and Italy, since the pilots would take place in the municipalities of Larissa and Rome, respectively. Furthermore, GDPR came into force on May 25, 2018 and consequently the processes of data collection, storage and processing were reviewed to ensure compliance with the provisions of the Regulation.

Another issue that primarily affected the self-healing functionality was the reluctance of the pilot LPAs to give extensive access to their systems. This was mainly due to security-related regulations and liabilities they were bound to, nevertheless, the human nature itself also seemed to affect it to a certain extent. Namely, despite the fact that the self-healing module could be configured to interact directly with a wide range of systems and thus offer automated reactions to the discovered threats (to the best possible extent), the pilot LPAs' system administrators seemed to want more control over anything that would happen to their system. This led to modifications in the user interface, to introduce the functionality of approving the suggested actions before they were actually launched. As a consequence, the self-healing functionality would operate in a supervised manner.

3.4 Interface design for increased awareness

In this Section a detailed account is given about the evolution of the user interface, starting from the initial ideas and thoughts about how it should look like for conveying awareness to the user, on to the various transformations it underwent according to the user feedback that was received in several iterations.

3.4.1 Initial thoughts on conveying cybersecurity awareness to the user

After having the first workshops with the participating municipalities, it became evident that for the end users the visualisation interface should feature a consistent and simple overview that at the same time could convey a high level of information. In this way it was anticipated that the visualisation scheme would be able to convey an equally high level of cybersecurity awareness, thus satisfying the primary requirement of the project.

The visual approach should also help categorise the threats into groups, as well as showing the number of threats and their criticality. To make it easier to follow trends, it should also incorporate visualisation changing over time. All the aforementioned functionality was chosen in order to raise awareness of the cyber security threat level.

For visualising threat levels, it was also early decided to use common colour schemes, similar to the ones used in other fields, so that threat awareness would have a common ground and would be intuitively understood by the end user. The following schema was chosen using the colors green, blue, yellow, orange and red in increasing order of severity.

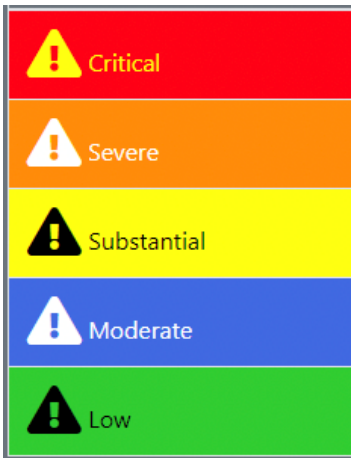

Figure 3.2: The 5-scale severity levels.

For visualising the threat levels, a circular graph similar to a dartboard was used, where the threats were shown in groups and their current prevalence was depicted via the size of the arch they expand upon. In this way, any number of threat groups could be shown, and it would be easy for a system administrator to pick out the most dangerous threats, to see which should be dealt with first. The “bull’s eye” in the centre of the disk indicates the overall risk level.

Together with this “dartboard”, a list of the top threats is shown, to provide more details about the individual threats that have been identified. Once a threat is selected, a modal window appears, where more details are displayed and through this window the handling of the treat is done. This design was meant for making it simple for the system administrators to handle the threats discovered by the CS-AWARE system.

3.4.2 The evolution of the interface according to user feedback

The initial concept of the user interface emerged quite early in the process. The very first draft of a potential visualisation scheme was presented in the Vienna consortium meeting, in February 2018 (Figure 3.3).

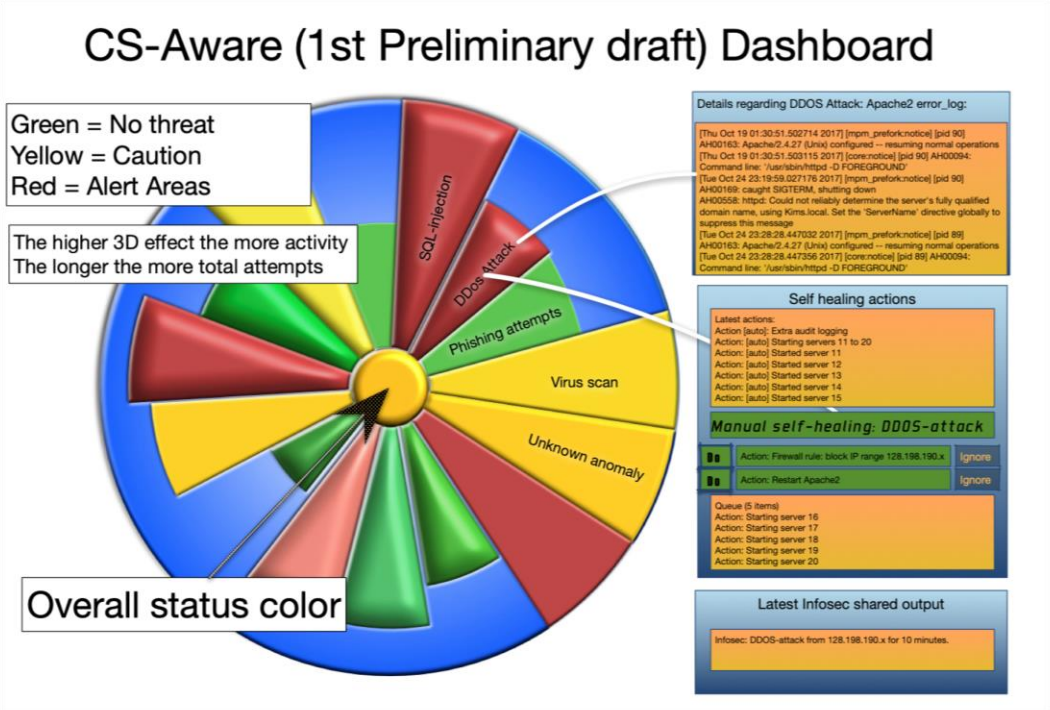

Figure 3.3: The first draft of the visualisation scheme (February 2018).

A few months later, in the Thessaloniki meeting (October 2018), the first graphical version was presented to the consortium members (Figure 3.4).

After development of the modules and at the preliminary stages of the integration phase, it was possible to have the first version of the CS-AWARE system, where all components could successfully communicate among them. Feedback from both the consortium members and users, indicated the need for exploiting the system dependency overview captured by the Soft Systems Methodology workshops (that took place in the municipalities) and stored in the GraphingWiki tool. Using this information would enable the system to show where the threat was initially discovered and what neighbouring systems could be affected by it. Hence, the interface was further revised and refined and reached the following look by the mid-term review meeting in Rome (April 2019).

Figure 3.4: The first graphical version of the visualisation (October 2018).

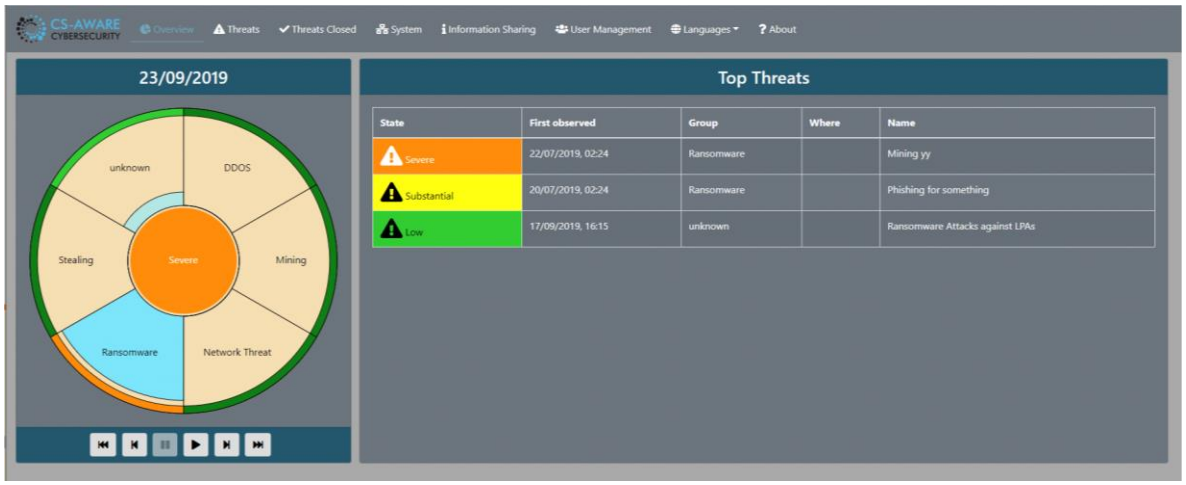

Figure 3.5: The CS-AWARE interface by the mid-term review meeting (April 2019).

Clicking on the "System" menu button, would open the system graph window, where the administrator could understand very quickly at which network node the threat was detected and which ones could also be affected by it (Figure 3.6).

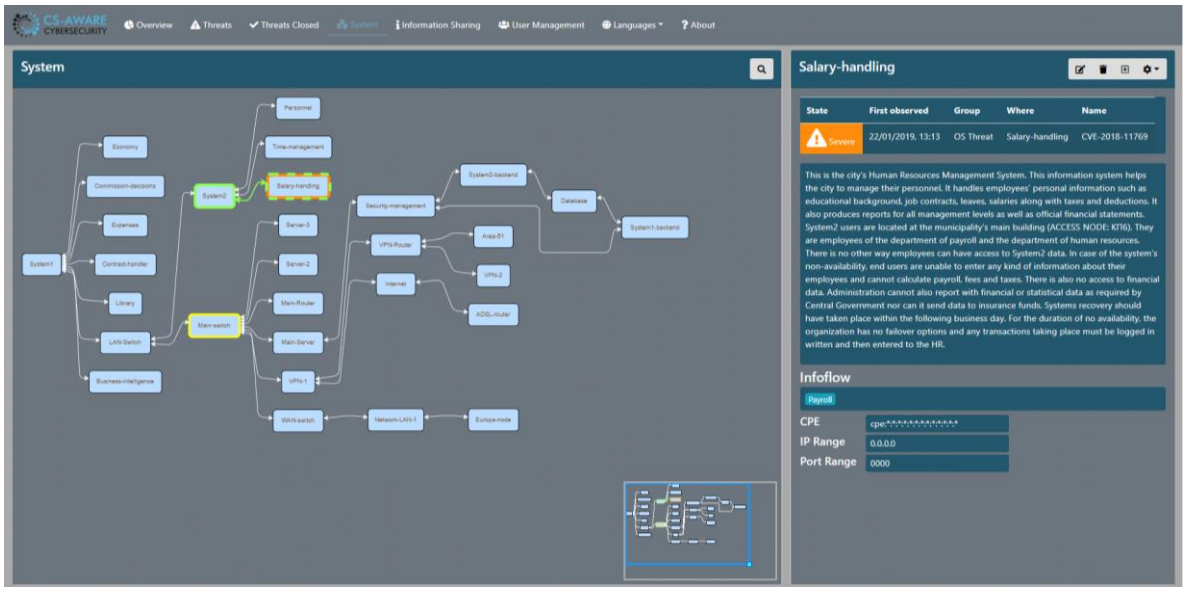

Figure 3.6: Visualisation with incorporated system graph, showing the various system nodes and their interconnections that could also be affected by the same threat.

Additional user input led to the expansion of the workflow engine, small changes in the colour scheme (for consistency reasons), enhancement of the system graph to show different symbols for different types of entities and changed the grouping in the dartboard overview from threat groups to IT categories, to provide better awareness for the system administrators. The treats and the nodes of the system graph were enriched with additional detail, so as to provide more information to the end users and help them understand the problem better. Finally, search functionality was added to the system graph and keywords were added in the social media overview.

3.5 Conclusions

This chapter presented the various stages during the development and implementation of the CS-AWARE solution, a system meant for raising cybersecurity awareness. For raising awareness in an effective and efficient manner, significant effort was put on threat contextualisation, so that the detected threats were correlated and filtered according to the particular qualities of the monitored organisation. Through the application of the Soft Systems Methodology, a detailed mapping of all nodes worth monitoring was created and this information was made available to other modules so that they were able to produce more targeted outputs, with the common aim of raising awareness as much as possible.

Each of the various components comprising the CS-AWARE system plays a particular role in raising the awareness of the end user, who is expected to be an IT system administrator. More specifically, the data analysis component has the ability to combine input from multiple sources (log files from the organisation's nodes, external cyberthreat intelligence, posts on social networks), analyse it and show what is happening (via the visualisation component). In this way, the cybersecurity awareness of the system administrator is increased, as they gain insight about cyberthreats that have affected or could affect their systems. Hence, the analysis results

are very refined, since both the importance of a given node and the severity of a threat has been taken into account.

The cybersecurity information exchange component also helps in raising cybersecurity awareness, by gathering cyberthreat intelligence from a world-wide spectrum. Presenting this knowledge to a system administrator can show them what the latest trends are, how sophisticated malware can act and spread, and so on. This knowledge itself can be an eye-opener, since it can help administrators to think like attackers or malware writers, which in turn can lead to improved procedures and measures that better protect the information system.

Finally, via the multilingual semantics support component, the language barrier was eliminated, thus enabling system administrators to understand better the outputs of the CS-AWARE system (both textual and graphical). Hence, this minimised the possibility of misunderstanding something or not paying the necessary attention to a detected threat.

4 Cybersecurity Awareness in Rome and Larissa: before, during and after CS-AWARE

Massimo Ferrarelli, Arianna Bertollini, Omar Parente, Claudio Ferilli (Roma)

Thanasis Poultsidis (Larissa)

Jerry Andriessen, Thomas Schaberreiter, Alexandros Papanikolaou (Editors)

4.1 Introduction

We present the viewpoint of the users of the CS-AWARE technology, the pilot municipalities of Rome and Larissa. This viewpoint has in part been elicited through stories and workshops, and in part is directly written in the text of this chapter. Users address their motivations, their objectives, their expectations for the CS-AWARE system. Crucially, the present the main impacts of their participation in this project: increased reflection, increased understanding of their own context and system, increased teambuilding and collaboration, and collaboration with academy.

Thanks to the expansion of digital technologies, municipalities are becoming intelligent, allowing the interconnection of systems, people and devices to improve infrastructure, efficiency and advantage for residents. Many local authorities have started investing in smart skills and are evaluating how they can leverage them to improve services and reduce costs. However, the benefits of technology can also pose dangers for townships. The use of Internet-connected systems and the offer of online services increase their vulnerability to a cyber-attack.

Roma Capitale and the municipality of Larissa are part of this context, which in their digitization process feel the need to face the problem of adequately securing their digital services, systems and networks. . Hence their adhesion to the European project CS-AWARE to collaborate for a cyber-security platform development.

In this chapter the two municipalities report the experience and evaluation of their participation in CS-AWARE. and discuss how the project has changed their awareness of cyber security, the impacts on their internal organization by their collaboration in team building activities.

4.2 How the chapter was written

The chapter is conceived as a personal report produced by authors from the two municipalities, as a response to a set of structuring questions by the editors. What they wrote is included as personal sections, embedded in more explanatory sections where the editors provide background to the user experiences. Everything that is reported has been voiced by participants from the two LPAs. The information provided about the local context, the starting situation, ambitions, and impact are derived from minutes and reports of the CS-AWARE workshop sessions and team meetings in which they participated. Especially, the information that the users provided during a story telling workshop and during a deployment scenario workshop will be exploited. We briefly describe the context of these two workshops here.

The purpose of *the story telling workshop* was for the CS-AWARE project to get insight into experiences of the users (the system administrators, managers and citizen-users) about cybersecurity issues before the project. We wanted to obtain a sketch of typical cases of

cybersecurity dangers, and the needs, roles and issues of people dealing with these dangers in their professional contexts. This was a necessary asset for our project, because no technology solution can be successful without considering user needs, in addition to involving the users in the design of the technology. We decided that the best way to capture experiences was in the form of a story. The story telling workshop involved small groups of participants from the municipality (system administrators and users from various departments) in collaborative efforts to produce meaningful stories about their cybersecurity experiences. The workshops were organised both in Larissa and Rome at the beginning of the second year of the (three year-) project. The procedure was generally as follows: Before these workshops, we asked participants through email to think about a personal experience with cybersecurity. During the workshop itself, users were asked to group into small teams that set out to deepen the content of these experiences according to a limited set of topics: the role of the organisation, the role of the system, the actions that were undertaken for resolution of the issue, the emotions of the user, and a conclusion providing perspective, e.g. lessons learnt, or things that could change. Then, we asked a representative of the group to present the story to all present. In addition to the project capturing these user needs, achieved by an analysis of the stories produced, the way we set up the story telling workshop also had a clear impact on the awareness of the users themselves, as they will recount below. We will report some examples of stories and some analysis outcomes that illustrate the state of cybersecurity in the two municipalities.

A year later, when the CS-AWARE technology was ready for deployment in the municipal contexts, we organised a *deployment workshop*. Users, together with researchers of CS-AWARE, worked for a full day on the creation of a deployment scenario, by collaborating in small groups. The main thrust of the workshop was to articulate and share local goals and expectations for deployment of the technology, on a shorter (during deployment) and longer (after deployment) term. This information was collected immediately after the third of the series of SSM workshops (Chapter 2), during which users were involved in discussing their network architecture, define critical processes, and symptoms of critical use cases, activities which were crucial for the design of the technology. The deployment workshop captured users' perceptions and expectations before actual deployment. The participation of the users in this workshop also served to raise their awareness about cybersecurity issues, and about what they expected of the technology.

To reiterate, the information in this chapter is based on outcomes of the story telling workshop (beginning of year 2), the deployment workshop (before deployment at the beginning of year 3), and on contributions by users (from the IT-departments of Rome and Larissa) written at the end of the project for the current chapter.

4.3 The experience in Larissa

The CS-AWARE project for Larissa began due to the very active EU-Projects department of the municipality. Our colleagues informed the IT department that a project called CS-AWARE was searching for pilot cities. After a short investigation, the IT team lost no time and in good collaboration with other members of the consortium, Larissa was in. That was the first step.

The project proposal was accepted. The project kick-off meeting was announced, and one member of the IT department was sent to Oulu to meet the other partners and to find out what exactly the project was about. The kick-off meeting was quite revealing, and outlined the

challenging requirements for participation of the piloting municipalities in the project. With tight time limits (only one month), the Larissa team then had to prepare the conditions and settings for the first SSM workshop. The Municipality welcomed the CS-AWARE analysis team and five full days of information exchange were devoted to the analysis of the municipality's systems. The Soft System Methodology was used in order to guide the amount of information. The IT department of the municipality, despite their deep and complete knowledge of its systems, learnt that it did not have a very high degree of sensitivity about security.

The next few months work was done on the clarifications of the network components and their role in the system. The CS-AWARE framework was ready, and we had to adopt it. This implied that we had to identify the critical points in our system. We had to write down the processes that include sensitive and critical information for the municipality. The CS-AWARE team worked on these tasks during the second workshop. In the next few weeks, the first testing application was installed in our systems and data was sent to the CS-AWARE repository for processing. The time had come to search into all these data and identify patterns. Suspicious behaviour, that our departments want to be aware of, since it indicates unusual or malicious acts. During the third workshop long discussions took place about patterns. Also, a big part of the third workshop was about the deployment plan.

Meeting by meeting, workshop by workshop, the project was evolving, and the IT department's security awareness was following, too.

4.4 Added complexity for Rome

The same series of activities were organised with Rome, but in a much more complex context. To deal with the workshop's organization a project manager has been appointed and a very heterogeneous working group has been set up. Colleagues with specific skills in terms of security were brought together with colleagues with skills related to European projects, IT skills, skills related to the management of economic resources. Altogether we required and assembled a wide variety of skills and competences, all within the Municipality of Rome. Furthermore, given the structural and organizational complexity of the municipal context, the participation of other staff inside and outside the administration was sometimes required, on the basis of issues and needs that gradually arose. It is important to point out that during the project we experienced various kinds of complexity: from administrative to technical, from organizational to cultural.

The workgroup – more or less stable due to resource turnover – was in charge of coordinating various activities, handling administrative matters, organizing workshops, participating to live and virtual meetings, presenting the project during several thematic events, updating citizenship on activity progress using Roma Capitale's web portal. The planning and the realization of a single travel or of a local event had to face a new approach, based on the confrontation with a variety of internal stakeholders and external partners.

Participating to CS-AWARE project was a great challenge for all of us, not without encountering difficulties mainly due to the fact that we were not immediately aware what final results would have been. Each of the involved stakeholders, including system providers, system administrators, managers, had to face a more flexible and unstructured environment, in which

the uncertainty about the results played a central role. This was not an ordinary, routine job: we had to deal with real innovation!

During first and second workshops, several application and infrastructure areas contact persons were involved to provide the necessary overview of our complex administration's functioning. In the subsequent workshops, due to other project partners requests, areas of interests were selected and studied in more depth, creating models using Soft System Methodology approach.

4.5 Cybersecurity awareness in Rome and Larissa before the project

The chance to participate in the European CS-AWARE project was perceived by Roma Capitale as an opportunity. Security in cyberspace is today one of the main needs for those working to guarantee community interests not only by ensuring a proper reliability of their digital services, but also by doing that in the most secure manner, in order to protect their data. Security's culture spreading is a must: both security and privacy must be adequately taken into account in all management decisions and actively lived: at the moment, the digital services *security by design* principle is not yet an integral part of our organizational culture especially if we consider it from our internal users point of view which still remains largely a "paper-based" one (but things are changing, maybe faster than expected!).

The municipality of Rome does not have a centrally organised and managed network of computers, software, databases, and services. The municipality is equipped with heterogeneous systems, not always interconnected, which give selective types of information to selected group of users only. Several providers work on logic, hardware, software, and perimeter security quite independently. Cybersecurity was a separate concern for each different provider. This is one of the reasons why different roles and objectives quite never match each other. We did not expect this situation to change, by participation in CS-AWARE, but we aimed for increased awareness on potential benefits for Roma Capitale's organisation.

A problematic aspect present before the project was a lack of awareness of the risks related to cyber security by most employees of the organisation, starting from the daily actions up to the management of external attacks. One of the most common duties worked on by employees is e-mail messages management which, even if it may seem trivial, hides many pitfalls due to lack of knowledge on dangerous messages and threats that can lead to security impairment of the systems. Another aspect relates to application services access management through weak passwords chosen by users who tend to select simple and plain words sometimes base on their personal interests or environment.

A story may illustrate this point: One of the tasks of employee E1 is to read all mail the mayor receives, which may comprise several hundreds of emails every day. Despite strict regulations, E1 opened an infected email. This mail had no subject, which could have caused suspicion. After E1 opened the mail, files in each directory on his computer he accessed became inaccessible. The IT-Department was notified, they discovered a type of ransomware that had encrypted all the files in the directories E1 had accessed. The computer was restored in the IT-Department, where all files that were not yet accessed were retrieved, and the system was reinstalled, and the intact files were restored. Infected files could not be retrieved. E1 was

initially terrified, feared the computer was lost, but now looks at it as a lesson to apply the rules more strictly for such cases.

The story is interesting because we should be aware there are persons for whom it is a duty to open all email. It also shows that these and other users may be very careful, but still occasional mistakes can slip through. The third interesting point is the role of the IT-Department: they solve the issues, but they also have strict rules. This may lead to users feeling insecure about the IT-issues they still might have.

So, a cybersecurity project aimed to enforce the awareness of the matter is fundamental to ensure in this way both security and privacy do become an integral part of the administration's culture path towards a complete digitalization. In addition to that, an effective data security policy is an absolute need in order to allow personalized services and data interoperability between our internal department and/or with external administrations, even more in a smart city perspective.

In **Larissa**, there is one system administration department for the municipality (including smaller municipalities around Larissa), where all cybersecurity issues are handled. System administrators in Larissa have different expertise, are aware of each other's competences, and regularly share information. Managers from other departments seem or need to be less involved. In **Rome**, there are many departments responsible for many services, making for a complex structure. Departments handling data or applications, or citizen internet services, do not necessarily share information on cybersecurity. It is unclear how and when communication between the various departments takes place. For awareness of cybersecurity, this means the information is highly *distributed*, and often unshared.

Developing more knowledge on cybersecurity is a local affair, and this may work fine in Larissa, but less so in Rome. Application of safety rules is monitored in Larissa by the system administration, although it is less clear if other department managers share this attitude. In Rome, if and how safety regulations are monitored, is highly dependent on the department managers. The role of system administrators is to help users, sometimes even helping them to avoid regulations.

Here's another story: This user works at a department responsible for managing European contracts. The problem that is frustrating our user, and probably many others, is that some websites from the EU are forbidden by system administration. On the other hand, many websites that are more dangerous are open for all, such as Zalando or Facebook. The procedure for employees is for the head of the department to write an official request for access to certain websites by certain people. This helps, but only for the people who have been listed in the request. For some people, phone calls can be a solution too. The issue is that some websites that can be dangerous are not closed for the employees of the municipality, while some websites who are well protected, cannot be visited. Even worse, the main website from the municipality is rated unsafe by most virus trackers, because it is not updated. All of this is interpreted as erratic by our user: is there any policy behind this?

The issue seems to be that the policy behind allowing or restricting websites within the municipality is unclear, and probably erratic, in the sense that it may be the result of many policies operating at the same time, including individual decisions. Consequently, some things are allowed, and some things are not allowed. For the user, this is highly unsatisfactory and

confirms a lack of trust, in addition to searching for individual solutions rather than for those that relate policy issues in general. There clearly is a transparency problem for the IT-Department AND for individual users.

The *rules and norms* that the IT-Department maintains underlying the regulations for monitoring safety behaviour, and providing services to the users, are different in the two municipalities. In Larissa, we see that the system administration expects citizens (internal users) to stick to the rules and regulations. Conversely, the citizens expect an immaculate and timely resolution of their cyber-issues. This means there is always a tension: trust may grow but also decrease. In Rome, there seems to be a general norm that the system is too complex, and we should accept imperfection to the extent that not all policy regulations are created in the interest of maximal cybersecurity. It looks like the various IT-departments are still able to provide quick services to users with problems. These services are provided on an individual basis, for a user who detects an issue, there is no follow-up, other users are not necessarily informed in case of a security issue. There is a lack of awareness about threats, especially in terms of understanding the threat and its possible impact on the system network. In Rome, this lack of awareness is related to the distributed knowledge of the complex system network: there is no single individual who completely oversees the whole network.

Concerning *sharing of information within the organisation*, in case of Rome, there is the issue of information sharing and knowledge management: knowledge is highly distributed and less shared, system users seem to have no concern for each other's cybersecurity issues, and the culture favours general regulations but individual solutions (not shared). For awareness, this creates a problem: it does not evolve nor spread. Also, in Larissa, while employees within the system department are aware of the cyberincidents that have occurred, this knowledge remains within the department, and seems of less concern for others, although the other employees that we met seemed to have some interest.

So, what can we assume about the status of cybersecurity awareness in the two municipalities before the start of the project? Awareness can refer to knowledge, but also to (the possibility for) action. In CS-AWARE, we think cybersecurity awareness originates in sharing and collaborating for understanding, not only a single cyber-incident, but also the context, the causes, and the possible impact. Although the situation in Rome reflects a more complex organisation for handling cybersecurity, underlining the importance for managing and sharing information, the main characteristics of how cybersecurity threats were handled in Rome and Larissa were (perhaps surprisingly) similar.

The perception of threats is not immediate, usually the system administrator is informed of an incident (by a service user, or a system alert), and some harm may already have been inflicted. Then, the system administrator must identify the threat, discover its possible impact, such as inferring when the issue probably appeared, in what part of the municipality network, or with which employees. Our impression is that the focus in both municipalities is on threat identification, and less on other processes that are part of awareness: threat comprehension, understanding of impact in the system network and its business processes, and decision making. We will explain this below. So, perception is not immediate, identification can be time-consuming, mitigation focuses on individual service users, and is local (part of the system), and not (holistic) system oriented.

For further understanding of the possible impact of a threat, if it is not already well known, a system administrator must access further resources for identification. Searching for and reading relevant and reliable information on the internet takes time, depending on the experience of the user, and often does not happen at all. The user may have to research log-files of the system, and maybe of services, to figure out what exactly is the problem. System administrators may do this, if they are responsible for the network or a part of it. If their role is to manage the database of a service, they may not be interested in such log files. In that case, communication with another specialist is needed, which requires information about the threat to be collected and understood.

For awareness this means that for a system administrator resolving a threat, full comprehension is not always necessary, and sharing information is only needed sometimes. Therefore, comprehension is limited, at the individual and at the organisational levels.

If the system administrator wants to understand the risks imposed by a threat to a system node, as well as to the other nodes, and which services will be in danger, a thorough understanding of the network as well as of the process in which the nodes are involved is a requirement (see Chapter 1). As awareness often is distributed, these aspects of resolution are a problem for users, especially in larger organisations. Users may be very knowledgeable for their own service but may not always oversee the possible implications for the rest of the network.

For awareness, this means that projection is local, and users may lack the knowledge to research their network. In Larissa, communicating with colleagues often solves the problem. In Rome, such communication may be more complicated, and requires the involvement of management and issue ticketing systems.

The final step in threat resolution is decision-making, and this involves several different actions. In the baseline situation, it usually means *resolving* the threat, for example by applying a patch or update, or blocking a user or part of the network. In a complex organisation, it may mean referring resolution to the expert responsible for that part or service in the network. In all these situations, experts, colleagues, including managers, may be informed, or consulted. This requires sufficient comprehension. Also, the user may need to ascertain that a threat is resolved. Most awareness in the base-level situation depends on communication between different stakeholders. In other words, awareness requires the collaborative attitude of equality of contributions, desire for sharing, and careful consideration of contributions by all.

4.6 Expectations of using CS-AWARE in Rome and Larissa

Roma Capitale and Larissa represent public administration of different size and complexity, but with the same challenge: to ensure the security of their growing number of data, which belongs to the entire population of their citizens, now and even more in the future, allowing a secure storage and exchange, preserving them from malicious or direct attacks. The data integrity and security are a prerequisite to protect their value and to share it among their citizens, also empowering the competitiveness of the cities in an increasingly data-driven economy.

The expectations of three groups of stakeholders (system administrators, managers, and local users) were collected before deployment of the software. Among other things, we addressed their objectives, what they expected the system to do, and how they expected their own

behaviour to change concerning cybersecurity. Participants had all been involved in the SSM design workshops, so they were already quite aware of the CS-AWARE affordances.

System administrators from Rome, currently people overseeing their own part of the municipal network and software, expected easy threat identification, preferably a trouble ticket on their mobile device, in case a threat was assigned to them. With that, they would like detailed information about a threat: type, time of incident, and all other information for better understanding of the threat. This would result in faster and more effective threat resolution. They would then expect to use the tool on a daily basis, and also be engaged in more reflection on past problems and solutions, and generally in more regular communication within the technical team and with internal users. Monitoring of incidents, and assigning (ticketing) threat resolution in Rome is and remains a management job, involving several people.

System administrators from Larissa, working as a team covering most of the municipality network, were interested in timely detection of threats, and absence of false alarms. They stressed the importance of trustworthiness of the information provided by CS-AWARE, and this information being up-to-date. The insisted on the system allowing them to decide, rather than relying on automatic system choices. They focused on learning by reflection and discussion. They expected to assign monitoring roles between them.

At the management level the differences between Rome and Larissa are very clear. The managers in Rome, who were directly involved in the workshops and design team meetings, focus on better collaboration within the municipality, between managers of the various departments, between managers and service providers, and with senior managers and users within the municipality. All of this may be realised on the basis of weekly incident reports and monthly trend reports, better quality of services and therefore more trust with the general public. There is clear awareness that this requires extensive discussions amongst policy makers.

The managers in Larissa were less involved in the workshops, or not at all. They expect the reputation of the information department to improve, and therefore general trust in system administration.

Finally, the users of the network and its services have an ambiguous role. On the one hand, they expect cybersecurity to operate without their awareness, and without their involvement. They simply want their system to be safe and reliable. Users in Rome were not interested in notifications about threats, especially not before they were resolved. In general, and this is the common situation probably everywhere, users are supposed to follow regulations. Users in Larissa said they appreciated some information about the threats that were resolved.

4.7 Outcomes

The main outcomes from the perspective of the municipalities includes aspects relating to increased reflection on cybersecurity issues in the organization, an increased understanding of the socio-technical structure of their organization, and the benefits from the increased internal team building and collaboration efforts within the organization and with academics. Those aspects will be discussed in this section.

4.7.1 Increased Reflection

It was clear that participation in project meetings, workshops and internal reflections in the context of CS-AWARE already had a great impact.

From the very beginning of the CS-AWARE project in Larissa, the initial task was to identify the persons to be involved from technical, users and managers perspective. All of them were about to be key players to the development, implementation and support of the project. After the work group was established, roles were assigned and the project could start for Larissa. The soft systems methodology was utilized for identifying the critical and sensitive points that the system should care about. Although the IT departments had deep knowledge about their infrastructure and software, never before were they triggered to spot the weak and sensitive points. Therefore, the next workshops proved very useful and training-like for the IT. The whole process changed the point of view of IT employees in Larissa, and created an improved security perspective about their systems. Companies and universities were directly in touch with the IT personnel and influenced towards raising the security awareness in Larissa. The collaboration between Larissa and the technical experts, security consultants and academics was constant and went both ways; both parts benefited from this part of the project, resulting to a better focused approach and final implementation specifically in Larissa.

In Rome, as the project produced its first usable results (i.e. graphical interface first demo in the second year of the project), we clarified, in the local deployment team, our ideas on what, till then, had only been abstract descriptions, concepts and questions becoming gradually simpler to understand and provide answers to different requests. This way of collaboration forced all of us, each for her/his part, to make an effort to identify elements that sometimes seemed obvious but actually are not. Furthermore, especially during workshops – when each contact person illustrated the part of her/his competence – different participants had the opportunity to listen and understand descriptions of activities, processes, area's difficulties different from their own getting an opportunity to know better the internal structure of the administration. Having such an overview will surely facilitate each of us in carrying out daily activities. All of this was even better understood by those who had access to the CS-AWARE web platform prototype, especially on system section tab where anyone can immediately get an idea of our local administration complex infrastructure's network, and, even more important, in asking critical questions, such as: How does a denial service attack may impact our organization? Or: How can we build effective knowledge management for collecting and comparing social media reports about new threats?

4.7.2 Increased understanding of the internal organization

Roma Capitale Digital Transformation Department's participation in the project certainly generated a greater awareness of cybersecurity in all employees, in particular it stimulated the curiosity of those colleagues who, by function, never had the opportunity to address these issues and provided an opportunity for deepening to all those who, on the contrary, were already aware of it, by work mission. Our experience in CS-AWARE project has shown us the importance of disseminating and growth of awareness of cybersecurity in our organization, not only in the ICT department, but in all the central departments and territorial structures ("Municipi", the fifteen municipalities in which Roma Capitale is subdivided). A possible organizational approach in order to spread and cultivate the new cybersecurity culture might

be to use the network of the local contact points for the digital transformation ("referenti della trasformazione digitale"): such a network, formed by 50-60 people with at least basic ICT skills and competencies, is already currently under training about the implementation of a new "digital workplace" concept, which has made mandatory after the massive use of remote working due to the CoViD19 emergency. Thus, we can suppose that also cybersecurity could play a crucial role in their training programs and in their hypothetical day-by-day operational mix in the articulate organization of Roma Capitale.

4.7.3 Teambuilding and internal collaboration

In Rome, the cross-cutting nature of the CS-AWARE project imposed a multi stake-holder approach which led the creation of a teambuilding practice never experienced before. The need to meet, discuss, create working groups with colleagues and technology's suppliers, relate to an international environment and collaborating with the municipality of Larissa, have certainly represented an enrichment for all of us both from a professional and human point of view.

A team made up of people from different backgrounds, subject matter, and mentality in their way of working is difficult to work with a smooth flow, especially if several members are participating for the first time in such a group. In the case of Larissa, a group of private and public employees was set up, without having taken part in such a large-scale program. Specifically, employees of the municipality of Larissa with the role of administrator in different computer systems of the municipality, suppliers who were invited to work for the first time in a public body in a European program, as well as people who were invited to work with the municipality of Larissa to improve security according to instructions from senior government agencies, they were key members of the Larissa team.

In Larissa, the cooperation of private sector employees with employees of the municipality in the framework of a European program on security, was an unprecedented undertaking which at least initially had some degree of difficulty. Until the start of the CS-AWARE program, the municipality of Larissa had experience with external partners, but only at the level of procurement or service. Never before have employees been asked to work with one of the municipality's associates to run a pilot project at European level. The difference in the objectives of work, the distance between them, the chronological deadline in cooperation with the other members of the program, and in general the difference in the way of working between the public and the private sector were a peculiarity which all parties were called to overcome in order to ensure the smooth cooperation between them.

In parallel with the program, the municipality of Larissa, following instructions from the Cyber Security Directorate of the Ministry of Digital Governance under the guidance of the European Union, was invited to introduce new GDPR rules for the management of the municipality's computing data. In this the managers of the computer systems of the municipality, who are also employees of the municipality, were invited to cooperate with a new DPO (data protection officer) from the private sector which in fact had no experience with any form of public body. The new DPO, of course, joined the Larissa team for CS-AWARE. Thus, in parallel with the project, the employees had to work with a new external partner, without knowledge in the computer structure of the municipality and the operation of the structure, in order to create and integrate these new security rules. This was an obstacle, since for several steps in order to complete the deliveries for CS-AWARE, the employees had to first consult the DPO, taking

into account the distance and the different objects of engagement. Nevertheless, the cooperation with the members of the Larissa team went quite smoothly resulting in the good operation of the team.

4.7.4 Collaboration with academics

Computer and network security is an increasingly important and complex branch of IT, especially with the new capabilities of computers and new forms of data sharing, processing and storage. Thus, understanding the concepts of security and techniques used to maintain the safe operation of computer systems in the municipality and other bodies is now of great importance. The academic offer in this case is very helpful, since the concepts and techniques of security are clarified and understood, which when applied in practice often are different from their theoretical approach.

The academic contribution has been of great importance and very useful throughout the project. The different approach, more theoretical and according to academic standards, helped to better understand the concepts related to security but also in general to the understanding of the entire computer security sector. The employees of the municipality of Larissa found quite useful the guidance given to them by the members of the project who have the experience in such large-scale cooperation in European projects. Applying security practices in day to day work, depending on the work objective of each employee, requires the knowledge of the proper tools but also the broader theoretical background that the academic approach can offer. After the project, now, computer security and problem solving in this area are more familiar in both theoretical and practical background, and are more effective in solving them following a multi-faceted approach - theoretical and practical.

4.8 Perspectives for the future

Without adequate security protocols and monitoring systems, civic authority's systems can be easily exploited by hackers by taking control of computer servers causing possible theft of personal data. To keep up with the cybercrime constantly evolving threats and tactics, municipalities like Roma Capitale must be proactive, not reactive, on cyber security. All this has led to an internal re-organization in order to create specific divisions designed to monitor and contrast any attacks with the support of technology.

One possible re-organizational scenario could be using dedicated people (adequately trained) for CS-AWARE platform monitoring able to manage different threats by themselves or by using system advice, maybe forwarding tasks to selected teams.

The CS-AWARE platform acquisition together with organizational re-engineering could bring benefits such as (but not limited to) easy identification and classification of the threat with decision support system for damage prevention; improved quality of the service which led to more satisfied citizens and personal data protection, hence increased trust in the LPA.

The CS-AWARE project brought several positive results for the Municipality of Larisa. Initially, it resulted in the creation of a tool that warns users of the application about security risks on the municipality's computer network. A tool useful for monitoring the safe operation of the municipality's computer systems and crucial in detecting electronic threats, as well as for informing any similar threats that had been dealt with in the past in one of the pilot

municipalities. Equally important, however, are the experiences gained from the employees during the project and from the cooperation with the team members, scattered in different regions of the European Union. These experiences involve both technical knowledge of the security of computer systems and networks, and how a program of this scope works in collaboration with its members.

The way a team of a European program operates is very different from the way in which the employees of the municipality of Larissa work on a daily basis. The number of members involved in the program, as well as the different subjects, the different working conditions, the different cognitive backgrounds that led to different approaches to certain issues and the different ways of dealing with the problems presented were unprecedented for the employees who participated for the first time in a project with so many participants from different places and with different work objectives, especially when these members came from places outside Greece with completely different mentalities.

This gave the employees the experience of working with universities and academics, members and shareholders of large companies and employees of a metropolitan municipality, that of Rome, which is very different from the municipality of Larissa. The behaviour of the other members in the discussions and in the adoption of the way they will work during CS-AWARE, their way of thinking, their acceptability in some cases where there were small difficulties that had to be addressed, or the establishment of common solutions to overcome controversies have left a fairly positive impression on officials. The way of thinking, which is very different from the one that was approached so far by various issues as well as the flexibility in adapting to certain situations, in combination with the above, are characteristics that the members of the Larissa team are willing to adopt in future collaborations.

Even for employees who had no background in computer science in general, the CS-AWARE project and their contact with its platform helped them understand security as a concept and why it is so important in the smooth running of the Municipality of Larissa. Understanding the concept of "awareness" is quite important in avoiding any infections from various threats, which users who have simply been asked to evaluate the ease of use of the application are now able to understand thanks to this project.

4.9 Aftermath

There are several ways in which the CS-AWARE system provides the user with possibilities for increasing awareness. Most of these possibilities are part of the threat detection and resolution process. More awareness by users could lead to changes in awareness by others in the organisation and to organisation change, if so desired, but obviously this is not an automatic consequence of more awareness.

Some of the main affordances of the CS-AWARE system are:

- It provides automatic threat detection and identification, and additional information about the threat from reliable internet sources
- It provides contextualised information by visualising the threat in the system network components and business processes

- If available, it provides suggestions for self-healing, that can be applied automatically (when authorisation is granted)
- It allows automatic sharing of cybersecurity information with cybersecurity authorities

This report of the municipalities (largely written by the municipalities) shows evidence of increased awareness linked to these affordances: threat detection, comprehension of dangers of threats, understanding of possible impact on the local network, understanding of the network itself, more collaboration and communication within and between departments, more awareness of the human factors in cybersecurity, and the awareness that much more needs to be done.

What any technology will not (and should not) be able to handle is the impact of awareness at the organisational levels. For cybersecurity as a collaborative activity of all stakeholders, communication between various departments is essential, as well as sharing of relevant information, and, crucially, a policy for knowledge management. While cybersecurity awareness may reveal the need for all of this, implementation of further steps can only be a slow process. CS-AWARE has given this process a big boost, which is all that we can hope for. Cybersecurity awareness is not a state, but an ever-ongoing process involving collaboration between all stakeholders.

5 Marketing a cybersecurity awareness solution in LPA contexts

John Forrester, Manolo Leiva Lopez, Massimo Della Valentina

5.1 Introduction

We discuss marketing CS-AWARE to the public sector. CS-AWARE is not a concrete product to sell, as in: here it is, there you have it. It is explained that the public sector is complicated, and heterogeneous in many aspects: size, policies, degree of autonomy and cooperation. Policy agents in smaller municipalities often lack the relevant knowledge, and often there is no explicit policy. For our context, we should link to the needs and expectations of potential customers. This asks for building good relationships and credibility. Various tactics for building up understanding and rapport are presented.

Marketing to the public sector is already a formidable task compared to marketing in the private sector. There are numerous rules, regulations, priorities and challenges to be taken into consideration. One-size-fits-all approach to government marketing does not exist given the differences in services supplied and agendas on the local level[1].

Issues like cloud computing, cybersecurity, and broadband connectivity are all issues of interest to all levels of government. Cloud computing, in particular, is a priority to government agencies, from local to national level. Some regions have even created their own clouds and in-house software firms to help manage their work. Cybersecurity follows closely as a priority with an-increasing awareness of ransomware and the vulnerability of cloud storage. Local government understand that broadband and Internet connectivity could potentially transform the lives of individual citizens and the community in general. Obstacles remain for anyone interested in selling cybersecurity to the public sector with the lack of resources in local government and the limited availability of qualified staff make it difficult[2].

Average population sizes of municipalities in Europe show that except for the Netherlands, Eire and UK, large areas of other European countries are dominated by small and medium sized municipalities who typically are suffering from a scissor's crisis with increasing demand for new and innovative social services and declining budget along with few qualified employees capable of handling cybersecurity software.

[1] https://modernmarketingtoday.com/glance-federal-marketing-space-exclusive-qa-alexandra-mchugh-new-relic/

[2] https://modernmarketingtoday.com/marketing-state-local-government-best-practices-strategies-work/

	Number of Municipalities	Population (2018)[3]	Average Number of Inhabitants per municipality
United Kingdom	419	65,648,054	156,678
The Netherlands	390	17,064,682	43,755
Ireland[4]	126	4,786,562	37,988
Poland	2,479[5]	38,131,648	15,382
Italy	7,958	60,589,445	7,614
France	36,658	65,129,822	1,776
Finland	313	5,534,655	17,682
Austria	2100	8,745,151	4,164
Germany	11,313	82,220,424	7,267
Greece	325	11,149330	34,305
Denmark	98	5,745,874	58,631

In recent years national governments in Europe have in recent years devolved a number of powers and responsibilities to local governments. In addition, there has been in many areas a push for more unions between local authorities to use more effectively the available resources. Indeed, in France, municipal cooperation is a crucial part of the national government strategy, considering the large number of "micro-municipality". Practically speaking in every country, given the reductions in funding and support, local authorities do not have any really real alternatives other than collaboration with others.

A cybersecurity campaign could be developed to focus on a selected number of regional and provincial institutions or with Unions of Municipalities, or at least one of the Metropolitan areas. Each in turn would involve their network of institutions. The strategy behind any

[3] Statistics taken from the Eurostat site and Comuniverso.it site

[4] 31 municipalities and 95 municipal districts for a total of 126 municipal entities

[5] 2,060 are classified as cities

eventual marketing activity could follow this process of "indirect dissemination" through larger organizations and a selected number of government associations in each country. In other terms, the dissemination models will differ from country to country, depending on both the systems of government and the interests of the stakeholders[6].

The total population of Italy is 60,589,445 (Istat 2017). The total number of municipalities in Italy is 7958 (Feb. 2018) The average resident population in Italian municipalities is 7,614 inhabitants. Some 5,541 municipalities have less than 5,000 inhabitants; in other words, around 70% of Italian municipalities are very small in size. Typically, their budgets are limited and have few qualified staff available. The smaller municipalities often have to share their staff with other municipalities. In recent years, many municipalities have begun pooling their resources trying to meet the increasing demands for public services.

Currently there are 537 active Municipal Unions (called: Unioni di Comuni) with 3,095 municipal members, that is, approximately 39% of the total number of municipalities. Only 17 of these Unions have more than 100,000 inhabitants. 8 big municipal unions associate more than 20 municipal members. One target for the cyber-security campaigns could be the 12 municipal Unions that have more than 16 municipalities as members. It is also possible to consider as a target the 96 municipalities that have the status of provincial capital.

Using the site for demographic statistics (http://www.comuniverso.it) 14 metropolitian areas can be identified in Italy. According to Wikipedia, Metropolitian areas usually refer to a region consisting of densely populated area and its surrounding territories, sharing industry, infrastructure, and housing. As social, economic, and political institutions have evolved over time, these metropolitan areas have become key economic and political regions.

The 14 Italian metropolitan areas are the following:

Regione	Città metropolitana	Comuni	Superficie (kmq)	Popolazione (Istat 2017)	Densità demografica (ab/kmq)
Lazio	**Roma**	121 Comuni	5363,28	4353738	811,77
Lombardia	**Milano**	134 Comuni	1575,65	3218201	2042,46
Campania	**Napoli**	92 Comuni	1178,93	3107006	2635,44
Piemonte	**Torino**	316 Comuni	6827,01	2277857	333,65
Sicilia	**Palermo**	82 Comuni	5009,28	1268217	253,17
Puglia	**Bari**	41 Comuni	3862,88	1260142	326,22
Sicilia	**Catania**	58 Comuni	3573,68	1113303	311,53
Toscana	**Firenze**	42 Comuni	3513,69	1014423	288,71
Emilia-Romagna	**Bologna**	55 Comuni	3702,32	1009210	272,59
Veneto	**Venezia**	44 Comuni	2472,91	854275	345,45
Liguria	**Genova**	67 Comuni	1833,79	850071	463,56
Sicilia	**Messina**	108 Comuni	3266,12	636653	194,93
Calabria	**Reggio Calabria**	97 Comuni	3210,37	553861	172,52
Sardegna	**Cagliari**	17 Comuni	1248,68	431430	345,51
Totale		**1.274**	**46.639**	**21.948.387**	**470,61**

[6] Kresl, Peter Karl and Daniele Ietri. Regional Studies Association: The Global Forum for City and Regional Research, Development and Policy. Regions and Cities. Routledge, New York, 2016

The metropolitan city of Roma Capitale, of course, is the biggest one. These 14 metropolitan areas will be important, given the number of municipalities (1274) and residents, as possible targets for anyone interested in marketing cyber-security solutions to local governments[7].

Since most metropolitan areas include multiple jurisdictions and municipalities (note the 121 municipalities associated with Rome), the metropolitan areas in EU countries will be of clear interest in terms of dissemination and marketing possibilities.

Aside from metropolitan areas the comuniverso.it site mentions that there are approximately 90 municipalities that are not provincial capitals and have more than 50.000 inhabitants. Those municipalities with more than 50.000 inhabitants are probably the most likely to have the social and economic resources to be interested in what the cybersecurity solutions. As noted elsewhere the majority of Italian municipalities are small and lack the resources to be able to manage a cybersecurity application by themselves. The situation does not change substantially in other EU countries. The majority of municipalities in the EU are small and medium sized in population.

With the encouragement of central government many municipalities are pooling their resources to be able to meet increase public demands for expanded public services8. Currently in Italy there are 537 municipal unions with 30,095 municipal members, that is, approximately 39% of the total number of municipalities. Only 17 of these unions have more than 100,000 inhabitants. Eight municipal unions have more than 20 municipal members. An obvious target for marketing solutions will be the 12 municipal unions that have more than 16 municipalities as members.

There are two issues to consider before beginning to plan a marketing campaign. First, it is important to remember that potential customers need a lot of education and guidance to understand cybersecurity in general, the threats they face, and what solutions might help them. This is particularly true of "policy" figures in local government who are not generally well versed in cybersecurity and are often unaware of how cybersecurity can be a critical part of the general preparedness plan of any government agency. Secondly, many agencies do not prioritize cybersecurity. There is plenty of evidence to show that cybersecurity is vitally important for protecting data and privacy. Unfortunately, many do not give much priority to security issues until it is too late. The need to prioritize cybersecurity needs to be carefully explained without resorting, necessarily, to lists of potential dangers and terror tactics. Warnings of potential doom rarely sell much, no matter how well intended the message is.

[7] Those municipalities like Rome that are the administrative centres of metropolitan areas have a responsibility for helping other municipalities in their efforts to promote digital transformation. Due to the lack of resources and budget many activities have been slow to develop. A well-planned cyber-security campaign that offers assistance and support could develop some interesting leads to potential customers.

[8] This is a trend occurring across Europe in recent years as central governments have turned to encouraging local autonomy and greater association between local governments as a means of alleviating budgetary problems.

5.2 Marketing strategies

The most effective strategy to use in the public sector is that of Inbound Marketing which is a business methodology that draws in customers by creating valuable content and experiences tailored to them. While outbound marketing interrupts your audience with content they don't always want, inbound marketing seeks to create connections to what they are looking for and solves problems they already have[9]. It is important to remember that while each of the tactics that will be explored below can certainly be implemented independently, they are far more compelling when used together. Together, they comprise the practice of what is called now "inbound marketing". Originally developed by Hubspot, inbound marketing is the latest form of marketing, and it has proven to be generally successful. While traditional forms of marketing consist of bringing your product or services to potential customers and fighting for customer attention, inbound marketing is more about letting your customers find you[10].

While inbound marketing is about drawing customers to your company, outbound marketing is about your business pushing its message out to the world, usually through advertising. Pushing your message in front of potential customers through outbound marketing can be costly. Buying advertising is rarely cheap, and results can be elusive since consumers tend to ignore ads. In contrast, inbound marketing can be low cost or even free, and because you are forming relationships and links, you are also building a lifetime value of your customers

This relationship building in the context of the public sector is best achieved through a variety of tactics and strategies. Examples would include whitepapers[11], video tutorials, webinars, podcasts, and social media posts. If the content you make available benefits the customer, they will be more motivated to buy. Particularly in the public sector, inbound marketing requires time to develop good content, nurture customer leads, and create "evangelists" for your company.

Reliability and credibility are, of course, important in every industry, but it's particularly important for cybersecurity companies operating in the public sector. This is because their potential customers are not only looking for a good solution to help them expand and improve their services, they are also looking for solutions that will help them protect their core mission of delivering services to their communities – ultimately, there is much at stake when it comes to choosing from myriad of software solutions on the market. It is not enough for customers to trust that a solution might be generally good; they also need to know that it will help them.

---

[9] Much of the material concerning "inbound marketing" strategies is based on suggestions outlined in ***https://www.ranky.co/growth-hacking-and-inbound-marketing-blog/digital-marketing-strategies-for-your-cybersecurity-company***

[10] ***https://www.hubspot.com/inbound-marketing*** One of the classical internet sites about marketing. Despite the volume of material and suggestions the basic message is really quite simple – keep it simple, unique, and direct.

[11] A white paper is generally perceived as "an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision" .**Wikipedia**

Understanding customers is important to recognizing the security issues that affect the public sector the most. Creating carefully crafted buyer personas (representations of customers based on actual customer data and market research – is probably the best strategy for acquiring a deeper customer knowledge and marketing to each of them appropriately.

For instance, IT staff may follow social media, but they are not involved in the decision-making process, in terms of finding suppliers. If we are speaking of an antivirus below 50€/year they generally have the autonomy do choose an antivirus, but the costs of the CS-AWARE platform is far too expensive. It becomes an issue for the policy branch..

The marketing and selling part must be basically done for the political side: the IT staff will oversee making it work.

When dealing with Managers or Directors of a department, chances are higher that the Mayor will follow his advice. But, it is rarely clear whether an investment in a social media presence in the market, other than providing a reference point for the company, will be efficient or effective enough to target the appropriate "decision-makers". At least in Italy the average age of a Manager or Director in the LPA is rather high and combined with an inconsistent use of social media by employees to promote and find elements for their relative jobs rather complicates the issue.

LPAs are just a little microcosm of the PA. The only huge difference is that in LPAs most of the decisions are politically driven: it means that, if you want to sell, you need to have direct contacts.

The environment around most LPAs has a strong territorial affiliation, in terms of politics. It is rare to find someone not politically aligned in an LPAs with the respective governing Party.

In this context, if we want to underline the real difference between the overall public sector and the LPAs in the Italian market, is its permeability. The general public sector (that reaches from a Ministry to the Postal service) can be entered (commercially and not) through a transparent process, according to the "transparency rule"12.

Marketing wise, with LPAs you are obliged, as a seller, to be in a relationship with the political counterpart. Of course, everything is conducted within a fairly well-defined legal framework. Not a single LPA will be interested in buying a product if you do not have a relationship with corresponding political elements and a good product13.

In 2003, the Italian Public Administration e-Marketplace (MePA) was introduced: it is a procurement platform managed by Consip SpA on behalf of the Italian Ministry of Economy and Finance (MEF). The MePA14 is a digital market in which any PA can purchase goods and services offered by suppliers, for purchases below the Italian threshold (at the moment 150 thousand euros). It is open to qualified suppliers according to a non-restrictive selection criteria.

---

[12] https://www.altalex.com/documents/news/2015/02/19/il-principio-di-trasparenza-dell-azione-amministrativa

[13] In recent years much progress has been achieved in reducing corruption but the association with political parties remains a problem.

[14] https://www.acquistinretepa.it/opencms/opencms/

The whole process is digital, using a digital signature to ensure legal compliance and overall transparency of the process. It works just like a real market, as the same products can be found and sold by different suppliers at different prices, terms and conditions. Suppliers can decide on the geographical area in which the delivery of their products / services will take place.

The rules that suppliers must follow to register and sell to the MePA are established by Consip according to the different product categories. MePA connects thousands of public bodies and suppliers distributed throughout the Italian territory, both centrally and locally. Registered purchasing administrations can use the two purchasing administrations. Consip also defines the qualification requirements and terms of service conditions. In this case, in addition to having to provide the service completely (information and contractual conditions included) in Italian, in order to be able to register as a supplier to the MEPA, the company must have a VAT number registered in the Italian chamber of commerce, for that it must open an office in Italy or it must be a company already present in Italy

From 150.000€ or more you need to be a different type of supplier (partizione gara d'appalto15) or participate in a public call (until the end of July 2021, after which the amount will be reduced to 40.000€)16.

Generally, there are two scenarios that follow:

First scenario: direct selling below the threshold of 150.000. Usually quite fast and functional, you sell your product and that's that. You follow the marketing tactics and advice listed above, particularly, in relationship with LPAs.

Second scenario: participating in a public call but in 99% of the time, they are hard (or almost impossible) to win. Proceedings are extremely bureaucratic, expensive, and long. Unfortunately, the bureaucracy is still geared largely to respecting the form rather than considering what needs to be done.

When dealing with customers, you should always remember that your customers are not the cybersecurity experts – you are. That means that rather than offer them the solution, you think, they have always been looking for, you should take the opportunity to educate them about newer, better solutions that they themselves might not have thought about before. Take the time to understand the security needs of prospective customers in the public sector, and offer them clear advice and insights based on their needs, it will help you establish your credibility, encourage customers to engage with you even more, and retain a base of loyal customers[17].

Applying an inbound methodology is great way to reinforce your message through the building of more lasting relationships with possible customers. It shifts the focus to valuing and empowering potential customers to achieve their goals at any stage in their journey with you. This is exactly why it is so critical to provide content that offers users added value--whether in the form of blog entries, helpful articles, social media posts, or an informative website. When

---

[15] https://www.sentenzeappalti.it/2018/06/29/frazionamento-artificioso-dellappalto-per-evitare-la-gara-integra-reato-di-abuso-dufficio-art-35-d-lgs-n-502016/

[16] Many believe this will be changed closer to the date.

[17] *https://www.hubspot.com/inbound-marketing*

you let possible customers find you, rather than constantly seeking them out, you tend to end up with more qualified leads and earn the credibility and trust you need to establish yourself as the leader in your area.

This is where customer relationship management, or CRM[18], software can be invaluable..

A CRM can help to::

- **Identify leads**: CRM software tracks actions taken by prospects, such as how often they open your email or visit the website. Use this data to segment prospects in the CRM so you can know which to pursue and which are unlikely to turn into leads.
- **Track your leads**: Your business requires a way to track prospects who have provided contact info. Housing this information in a CRM makes it easy to track who requested to learn more, and who needs some follow up to close the sale.
- **Use automation**: Sending email follow-ups is a good tactic, but without automation, this task can be difficult to manage efficiently[19]. Many systems provide capabilities to send automatically emails, and to schedule these emails to go out at regular intervals.

The unified view of your customers offered by CRM software serves as a repository for all customer data. This single view of the customer ensures they have a seamless experience when engaging with your company, even if different employees handle each engagement[20].

5.3 Building credibility and trust by creating comprehensive and data-driven content

The most important issue for the marketing of cybersecurity solutions is the quality of the content being offered: an effective presentation can be more effective than other instruments for promoting more education and awareness of the issues on the part of potential customers[21]:

- **Improve the "content"** this shows what you want to offer is important to building your credibility
- **Old themes about costs and dangers** are problematic and, very often, counterproductive. Different angles on the types of cyber threats and how they relate to what you offer can be far more effective in the long run.

---

[18] An eventual choice of a CRM is beyond the scope of this chapter. It is well worthwhile to research the variety of CRM systems, particularly the open sourced one on Linux. It is not clear the scale of your activities are or will be in the short-term, the best advice is to keep it simple and identify a CRM that is flexible, easy to maintain, and open source.

[19] Avoid where possible general impersonalised emails. Take the time to learn how to merge lists of names and addresses with text.

[20] https://www.dealsinsight.com/inbound-vs-outbound-sales-what-is-the-right-and-powerful-choice/ As they point out in this post, well-constructed and focused email can elicit a better result than social media. Potential buyers are interested in credible solutions that focus on what is being offered and how.

[21] https://www.sevenatoms.com/blog/cyber-security-marketing-tactics-that-actually-works

To start with you need to figure out your objectives for content marketing looking at why you are doing this at all? What is content going to do for your organization? Will it create more awareness? Can it generate more leads? Would it be useful for improving loyalty and client retention?

An important point made by many is that it is not enough to be good at content marketing. Your goal needs to be good at business because of your content marketing.

As you develop your content marketing program you should think of "what sets you apart?" why your solution and not another? There is an enormous amount of content in the market. You should ask yourself will it be useful to your customers. Will others see it as "motivational, inspirational, or otherwise?" What is the core of your content program?

"Your objectives dictate your metrics." If you want to produce awareness, try to measure that awareness.

Four critical metrics are often focused on [22]:

1. **Consumption metrics** the easiest to understand are those that answer the questions – how many people viewed or downloaded a specific content?
    a. **Page views are** relatively easy to measure with programs like Google Analytics or the like, but you need to take the "page views" in their context. By themselves they are not necessarily that significant in terms of what was achieved – views do not necessarily translate over time into sales..
    b. **Video views** can be seen easily on Youtube Insights or similar programs.
    c. **Document views** SlideShare, for instance, can facilitate access to data
    d. **Downloads** can be measured through your CRM or Google Analytics
    e. **Social chatter** there are various services available to measure chatter. Here too the context is important in order to understand the significance.
2. **Sharing metrics** how resonant is this content and how often is it shared with others?
    a. Measuring how your content is shared impacts two content goals **brand awareness and engagement**
    b. Metrics may include (to boost numbers)
    c. Like, shares, tweets, …make it easy to share
    d. Forwards your email and Google Analytics can help
    e. Inbound links
3. **Lead generation metrics** measuring these helps you answer the critical question "how often does content consumption result in a lead? This includes form completions and downloads, email subscription, blog subscriptions, and the conversion rate.
4. **Sales metrics**

22https://www.convinceandconvert.com/content-marketing/marketing-strategy-steps/

It is also important to research content needs – What do clients need to know at the various stages of their journey towards becoming a "buyer". Segmenting your audience may help define who you have as an audience and what the different needs are.

- **Different blogs** can be useful in reaching out and engaging prospective audiences. Whatever activity is chosen should be carefully followed and maintained. Nothing is worse than presenting out-of-date or misleading content to prospective clients
- **Terror tactics**, it is important to remember, they simply don't work in the long run; the effect wears off over time. Giving people real-life situations and questions to frame their thinking is far more effective in the long run - for example, discussion questions asking potential customers what security solutions does your agency really need?
- **Offering content** whether it's articles, links, or related white papers in download to support your offer is a great way to convince others to look more closely at your offer.
- **Offering content that can be downloaded** is a good way to convert curiosity into substantive leads.
- **Landing pages for content material** (where the material for download can be briefly presented) are useful for users to evaluate whether the material is of interest.
- **Case Studies** are also important for engaging those users who already have a good idea of their problems and what solutions will probably work best.
- **Videos** are also an excellent communication tool if planned well. Many executives prefer to watch a video to reading a text. Videos that describe a solution can be the best way to communicate what a cyber security offering does and why it could be useful to your potential customers. As a medium a video may be far more helpful for executives who need more education.
- **Webinars** are also an excellent means to engage with people who are already interested in your solutions. Presenting case studies of your solutions can be an excellent means to allow others to become better acquainted with what you offer as cyber-security solutions.

5.4 Email marketing

Email marketing can be an effective way of reaching prospective customers. and if done carefully, of cultivating leads and moving potential users further ahead. An important element, as always, is giving priority to creative and engaging content without exaggerating about what is being offered. Social media tends to be a difficult medium for creating authoritative content. Email allows one to control the message and be more focused. Ultimately, as noted earlier, it's important to improve your content, taking care not to resort to basically "worn-out" themes of impending dangers and doom but to focus on where customers might be in the process and offer them solutions. Awareness fostered through education and persuasion should be the focus of an email marketing campaign for cybersecurity.

You should always try to maintain connections with customers and others with carefully crafted strategies:

- Use well developed statistics, case studies, reports, studies, interviews, and the like that tend to provide readers with a more detailed understanding of important cyber security topics in your emails.
- Compile authoritative whitepapers on arguments of interest to clients.
- Ask clients for endorsements.
- Avoid the use of jargon (particularly English based)
- Develop informative content like blogs, downloadable material, webinars, and short video tutorials. Be sure to add links to information about recent attacks and security issues, particularly, where the sources break down complex cyber-security topics for a wider audience.
- Attach summaries of relevant articles from industry sources that help readers better understand hot topics in cyber-security.
- Use leaflets and other material to hand out to people at events or advertisements in print publications (while changing many in the public sector still use print material).

5.5 Try to educate your "bottom-of-the-funnel" leads with interactive sessions

Webinars can be one of the best ways for those in cyber security marketing to connect with bottom-of-the-funnel leads – those that are fairly far along on the process. A vital part of an effective webinar is the interactive element. It often includes a Q&A session at the end of the presentation that offers attendees the opportunity to ask questions about the topic and the services you are offering. The questions and concerns that users ask during the webinar are also good starting point for developing new content for your target audience. Attendees are already interested in learning more about your solutions and the threats it protects against, and they have usually taken time to do some research. This signifies that they are more likely to be engaged in the topics you are presenting. Therefore, this is an opportunity to advertise other helpful content or encourage demo sign-ups. Even if you decide to pre-record your webinar, you can still accept viewer questions and respond in a follow-up[23].

If you offer a webinar online, it is always a good to record the content. You can make the recording available later for people who were unable to attend.

If the webinar elicits a good response, then you may also want to use the topics discussed there and create other types of content like blog posts around these topics. In order to promote a webinar and drive attendance, paid channels like LinkedIn and Google "retargeting" ads to obtain results[24].

---

[23] (https://www.dealsinsight.com/6-powerful-cyber-security-marketing-tactics-that-actually-work/) In other words, clients already fairly sure of what they would like.

[24] Keeping LinkedIn entries and Google Ad Campaigns updated is always important.

5.6 Up your content strategy using paid campaigns

B2G[25] campaigns are good for accomplishing two important goals:

- They augment your content marketing efforts
- They also help you direct prospective clients to your demo landing page

Many are of the opinion that paid campaigns and inbound marketing are not compatible, particularly in the public sector. If you combine these strategies, you can manage to create a compelling campaign. For example, as noted in one blog posting from dealsinsight.com, posting study with some compelling data about a cyber threat. With this type of asset, time is of the essence – the older the material is, the less likely prospective clients will find it useful As noted before, updating material is critical when trying to attract the interest of prospective customers[26]. Posting and promoting content through paid channels can let others to see results more quickly.

One of the major goals of any B2G marketing is persuading prospects to request a demo. While moving prospects to this stage demands a certain amount of work and encouragement, paid campaigns can help accelerate the process for those who are ready to make a buying decision.

Some cyber security companies avoid using paid campaigns due to the competitive nature of paid advertising. Certainly, it is completely understandable. If you do not have a clear idea of what you're doing and what priorities you have, it's easy to spend thousands on cyber security ads and get little or nothing in return. Finding specialized help can be one solution but it can be rather expensive. At least within the public sector, networking can be crucial for anyone interested in marketing a solution. While public procurement is increasingly regulated within the EU, the competition is quite high and the marketplace is crowded with solutions.

5.7 Identify the decision makers who does what?

Identifying and understanding your audience is critical and should be the first step in developing your cyber security marketing strategy. To do this efficiently, many recommend creating "marketing personas".

A persona is nothing but a semi-fictional representation of your ideal client. B2G personas not only give a face to your target audience but also provide insights to help you decide which strategies will work best, how to communicate, which marketing channels to use and what kind of messaging will have the desired impact.[27]

---

[25] Business-to-government or business-to-administration is a derivative of business-to-business marketing and often referred to as a market definition of "public sector marketing (Wikipedia).

[26] https://www.dealsinsight.com/6-powerful-cyber-security-marketing-tactics-that-actually-work/

[27] https://www.insegment.com/wp-content/uploads/2017/12/inSegment-5-Successful-IT-Cybersecurity-Software.pdf Rather than focus on the technical aspects of the solutions InSegment cites

If you are marketing to local governments, you need to resolve problems facing local governments and their agencies. For instance, compiling blogs which focus on the high-profile cyber security attacks that have hit Deloitte or the National Health Service in the UKNHS may leave local governments thinking they have little to worry about. Like small-medium sized businesses (SMB) local governments are the weak point in the chain and many attacks are geared at them.

Creating 2+ personas to cover the different roles that you need to speak to will help develop a targeted campaign. The smaller municipalities will fewer staff. Campaigns usually need to be directed at the larger (medium to large municipalities). You will probably need to target both the IT and the Policy sector. It is always important to research your audience.

5.8 Focus on topics relevant to the range of vertical services involved

While "vertical marketing strategies" are commonplace due to their efficacies, many smaller cyber security firms still are reluctant to narrow their focus to a few key verticals for fear of alienating a potential prospect that does not fall within those parameters[28].

Instead, they may focus on the critical areas their solutions address across sectors and treat verticals as an afterthought. This approach does not generally stand out in the B2G cyber security space. Since most buyers of cyber security products work in the same areas, too many vendors end up sounding the same. Buyers of security solutions want "secure end-points, a secure network, the ability to detect a breach, secure software development practices, strong governance, remediation policies in place, and the ability to gain rapid insights when a breach does occur, to name a few"[29]. Also, with so many pitching their solutions, the cyber security sector can be noisy and confusing with little distinction in the messaging, which can swiftly become frustrating for buyers.

Marketers should focus on topics their prospects care about, relevant to each target vertical. If a target buyer is local government agency, focus on topics they care about, such as standards and norms in their different areas (health, social services, housing, etc.). Discussions should always be framed around the buyer's perspective and relevant to their day-to-day operations.

5.9 Closing comments

Cybersecurity marketing can be difficult to grasp and to effectively employ the available marketing tools. The marketing agency inSegment outlined in an interesting pdf five campaigns that using skilful storytelling made a compelling and effective case for themselves. All the companies behind these campaigns selected in the article by inSegment are "unorthodox and,

---

the efforts of IBM to inspire its audience by creating digital "personas". Others refer to this as segmentation of the audience.

[28] https://www.insegment.com/wp-content/uploads/2017/12/inSegment-5-Successful-IT-Cybersecurity-Software.pdf

[29] https://www.insegment.com/wp-content/uploads/2017/12/inSegment-5-Successful-IT-Cybersecurity-Software.pdf

often, completely new methods to approach complex topics like AI and cybersecurity". They used inventive marketing techniques ranging from podcasts, documentaries, cartoons, and videos to attract interest. Certainly, using these tools requires, at times, significant resources to create a marketing campaign but they can achieve a excellent return. As inSegment points out "increased and higher quality leads generating loyal and long-term customers is just one of the many positives that a well-structured campaign can achieve for your business." With the growing numbers of businesses in cybersecurity, the industry is becoming increasingly competitive. Those who want to reach prospective customers in the public sector must become more innovative with their marketing activities[30]. It's your content that matters more than any particular tool or platform.

[30] https://www.insegment.com/wp-content/uploads/2017/12/inSegment-5-Successful-IT-Cybersecurity-Software.pdf

6 Outcomes of the CS-AWARE project and relevance for cybersecurity awareness in other contexts

Jerry Andriessen, Thomas Schaberreiter, Alex Papanikolaou, Juha Röning

6.1 Introduction

We summarise the outcomes of the CS-AWARE intervention in two municipalities. Because we collected their feedback during most of the design and implementation processes, users are strongly involved and have a sense of ownership. We discuss the 'awareness' concept in some detail, to conclude that many aspects of awareness have been evolving in a positive direction. We end the chapter with a short discussion of three domains for which our approach to cybersecurity awareness could also make a positive contribution.

6.2 Cybersecurity

During the final year of the CS-AWARE project, we deployed the system at two municipalities, and evaluated its use through several evaluation measures: workshops, usability testing by cognitive walk-through, and several questionnaires. In this chapter we provide a summary of the outcomes, especially pertaining to cybersecurity awareness, of our work with Rome and Larissa. We have already learnt from the pilots in Chapter 4 that they considered their increased teambuilding and collaboration as the main impacts of their participation in the project. Their mutual understanding with respect to cybersecurity awareness did not only increase by working with the CS-AWARE system, but especially from their participation in the workshops discussed in Chapter 2, which incited the collaboration within their municipal organisations. In this chapter we briefly review the outcomes of the project, in the light of cybersecurity awareness, and we provide some pointers to other domains and contexts in which our approach might be important.

The workshops. The interaction between workshop participants during the socio-technical system analysis (according to the methodology specified in Chapter 2) has proven to be a remarkably positive element in the creation of individual and organizational cybersecurity awareness. Throughout the workshop the users gained a deep technical understanding of their own systems and their security relevance, which simplifies the interactions with the technical part of the CS-AWARE system, since incidents based on behaviour monitoring detected by CS-AWARE are instantly comprehended and understood by users that helped to define them. Furthermore, since this analysis leads to system monitoring that the actual users and administrators of the system care about, an increased motivation to address potential issues detected by the CS-AWARE system could be observed.

Technology Framework. Piloting results have shown that the general framework presented in Chapter 3 works as intended, and the technical functionality of each component is given in the generic case, as well as in the two pilot specific examples in Roma and Larissa. We have not identified any shortcomings or misconceptions of the technical framework that would have necessitated a major revision of the implementation. This has been confirmed by functional testing as well as in the usability sessions with the users of the municipalities of Rome and Larissa. The positive outcomes have been confirmed by the evaluated results of questionnaires

in two piloting rounds, with all key indicators showing a positive result. The two advanced concepts implemented by the CS-AWARE interface, self-healing and information sharing have been received well by the users and the potential for inclusion of those functionalities in the day-to-day workflow has been confirmed. Because these concepts are relatively new for the two piloting municipalities, the time to get familiar with the relevant interfaces provided by CS-AWARE has been longer than for the other tested functionalities.

Usability. CS-AWARE is not a simple system to use. This is especially due to the nature of the domain: the complexity of information for cyberthreats (severity, possible impact, type of threat, part of the network compromised, further possible impact, etc.), the difficulty of comprehending this information (coming from reliable sources, but still compact and abstract), understanding the role of compromised software or technology in the context of the municipal network, and making the correct decision for threat mitigation and protection of the network and the citizens. Such is the work of professionals, and they cannot make mistakes without consequences for the network, departments in the municipality, and, ultimately, the citizens.

We have deployed and tested the system in the context of two municipalities, who have very different ways of working. In the municipality of Larissa, system administrators performed all the tasks, and consulted with their direct colleagues. In Rome, expertise was distributed, and various tasks and services where handled by different persons. The possibility of handover of threat information to other experts proved to be a crucial feature.

For these tasks, the system provides options. In various tests, users indicated that:

- The elements presented by the interface were clear, and their structure and functions were clear
- The elements were presented in a consistent manner
- The way the system works is easy to remember
- Working with the system does not require much help, with some time for learning it
- The presented information is complete, for making decisions
- The descriptions are clear and precise
- The system allows flexible use, users can go back and forth as they please, and retract most earlier steps or decisions
- The system presents the information in the language of the user, translations work well
- The options that the system presents are sufficient for acting

Through the usability sessions with the users in Rome and Larissa we could confirm that the awareness created through CS-AWARE, and visualized to the user through the CS-AWARE user interface, provides insights into the security relevant system behaviour, and provides the user with information that is currently not available through any other technical means. A clear benefit and potential for efficient reaction to and mitigation of security issues has been identified.

6.3 Awareness

We defined awareness as a concept with 6 components: *knowledge* of cybersecurity threats (1), knowledge of the system network (2), knowledge of the organisation (3), knowledge about external cybersecurity-related organisations and communities (4) as well cybersecurity *agency*: knowing how to act in case of a threat (5), and acting when there is no threat (6).

Agency can be defined here as the possibility for actively contributing to cybersecurity. It alludes to the capacity of humans to distance themselves from their immediate surroundings and it implies recognition of the possibility to intervene in, and transform the meaning of situated activities (Mäkitalo, 2016).

Concerning knowledge about threats (awareness component 1), we can say that much has changed. Instead of laborious sessions inspecting logs and internet sources, which were common practice before CS-AWARE, much of this is now handled by the CS-AWARE system, and in such a way, that reliable information about threats is readily and immediately available for the user. This means that potentially, threat awareness is increased. Users agree with this statement. Knowledge of threats is increased with every new threat, especially when users, in addition, are discussing the threat with colleagues and are sharing their experience with others, during or after threat resolution.

The knowledge by users about their municipal system network (awareness component 2) was already greatly fostered during the SSM workshops, taking place before deployment. We have evidence that the awareness ratings for municipal network visualisation and projection of threats has gone up during deployment and can therefore conclude that also system network awareness is addressed in a more than sufficient manner. We should note that the amount of work for constructing the network model, which involves mapping the network, including the roles of the various components in the execution of particular business processes, depends on its complexity and the knowledge of the system department. This complexity is greatly increased for larger municipalities. Also, the implementation of future changes in the network, for example when new components are added, needs to be paralleled by revisiting of the system visualisation and business processes.

It is clear from our evaluation that the CS-Aware System has, in the opinion of the respondents, significantly improved both their cybersecurity awareness and that of the organisation(s) in which they work (awareness component 3). Whereas in Larissa, the focus was on the increased quality (and therefore the reputation) of the system administration department, the focus in Rome was on improved communication and collaboration between the many departments involved in services to the municipality and its citizens. However, improvements are still possible in the involvement of management in cybersecurity at the organisational level, for example through the provision of regular system reporting, additional workshops, and training.

The level of external organisations, communities, or other departments involved in cybersecurity (awareness component 4), who all would have an interest in sharing information about cyber incidents, as it stands now, is merely a technical asset. Initially, information sharing was not seen as a major technological challenge, and the functionality provided by CS-AWARE fulfils the technological need. However, the possibility of sharing of security relevant information with parties outside the organization led to significant organizational and policy challenges that need to be solved first before sharing can become part of daily practice. This is

very important, as, due to the reporting obligations of the NIS directive and the GDPR, municipalities are currently under pressure to get the relevant policies in place to address security relevant information sharing.

We understand most about the awareness component of user agency for handling cyberthreats (5), because we undertook, with our users, a number of cognitive walk-throughs of the system, whereby these users had to think aloud while handling a (simulated) threat. When we say that CS-AWARE is an expert system, we crucially refer to the process of dealing with threats. This process was different in the two pilot municipalities. In Larissa, the system administration department handled all cyberthreats. This is a small department, with experts who can work together in order to resolve a threat. The way they currently work does not have to fundamentally change with CS-AWARE. In Rome, expertise on all aspects of the extended network of nodes and services, is highly distributed. Handling cybersecurity threats requires a central expert who delegates different tasks to different experts, who are responsible for their particular system or service. More often than not, handling a cyberthreat will involve more than two system administrators, who work in different departments. For the communication that this process requires, Rome already had a ticketing system in place. CS-AWARE is made to work in both contexts, so a ticketing system was implemented as well. These differences have implications for awareness and on how expertise is distributed between users.

We distinguished four main phases in the process of dealing with threats, based on the phases described in Hibshi et al. (2016): *Perception* (user perceives a threat), *Comprehension* (User understands the threat, its characteristics and information provided by the system), *Projection* (user foresees consequences of actions in context), and *Decision* (User makes a decision). From our evaluation of the results of usability tests, and from additional questionnaires users showed good awareness of these phases:

- Concerning *perception*, the opening screen of CS-AWARE provides immediate awareness of a threat, at least for users involved in monitoring.

- Concerning *comprehension*, we noted that users attend to the main characteristics of a threat (type, date, system component involved), but not always to all details (detailed description, system information and history). This may have good reasons, linked to a user's expertise, and the need for immediate resolution may require efficient handover. However, we observed that threat comprehension has more attention from those who are responsible for all aspects of threat resolution, than from those who deal with some part of that process.

- Concerning *projection*, the same applies as for comprehension. While some users study the network visualisation extensively, others do not look at it, and focus on their own 'section' of the network. It should be noted that the actual repair, by inspecting log files of the affected system component, still takes place 'outside' of CS-AWARE, except in the case of self-healing. We highly recommend training for new users to focus on projection of threats through system visualisation with CS-AWARE.

- Concerning *decision-making*, we noted that handover of threat mitigation to other users was the rule rather than an exception. Also, we noted that most users have the habit of

checking if their decision was implemented correctly (e.g. threat now listed in resolved threats, or handover now included in current threats). It was clear that this already was part of their normal routines, and now made explicit (and recorded) through CS-AWARE.

As a conclusion for agency in handling threats, as a component of cybersecurity awareness, we can say that CS-AWARE greatly facilitates user agency, making detection and mitigation more efficient and effective, with the additional asset of better comprehension and projection of threats. The extent to which comprehension and projection abilities of users increases, depends on the extent to which users pay attention to this information. The very positive outcome of the questionnaire seems to be relative to the roles and actions of users during threat mitigation. The more time the user indicated having spent with the tool, the higher the scores attributed to awareness of all aspects of handling threats.

Finally, how about user agency when there is *no* immediate threat (6)? System administrators in Larissa have been 'playing' with CS-AWARE when there were no threats to resolve. Of course, this is an important activity for gaining experience. System Administrators in Larissa stated their ambition for learning in the deployment scenario. They had an interest in an improved reputation for their department, as a consequence of improved services. This could lead to considerations about weaknesses in the network components and development of new services for citizens. On the other hand, in Rome, ambitions were formulated at the management level, in terms of more and more effective interactions between departments in the context of cybersecurity. Although the managers in Rome were very positive about possible organisational impact (see the next section), it remains to be seen how these expectations will be realised.

Concluding, through deployment of the CS-AWARE system, we can say that cybersecurity awareness in both pilots has been greatly increased, at the level of threat detection and mitigation, and, to a somewhat lesser extent, to understanding and learning about threats, also in the context of the system network. Further work is expected, after the project, for the exploitation of increased organisational awareness in both municipalities, and the elaboration of sharing threat information with relevant external agencies and authorities.

6.4 Other Applications for cybersecurity Awareness

CS-AWARE is not only a system, it is also an approach to cybersecurity awareness. While the systems that we built, with significant user input, can be applied to similar context, i.e. other municipalities, we can also envisage other domains or contexts within a local government context, and perhaps also in other contexts. We end the overview of CS-AWARE project with two contemporary and relevant examples for which our approach seems valid as well: smart cities, e-governance.

6.4.1 Smart City Applications

One of the major emerging technologies in the context of LPAs is without a doubt the continuing digitization of administrative services commonly referred to as "smart city". For example, our partner city Rome has a wide ranging and long-term strategy of implementing smart city capabilities in the context of the Roma Data Platform (RDT).

Considering the growing demand for innovative IT tools, Roma Capitale decided to customize and implement a Smart City Strategy aims at increasing efficiency and effectiveness of interactions with citizens as well as monitoring the level of services provided. As depicted in Figure 6.1, the smart city strategy will be implemented incrementally, starting with various applications in Education, Taxation and Reports/Complaints, but aims at integrating virtually all administrative areas over time.

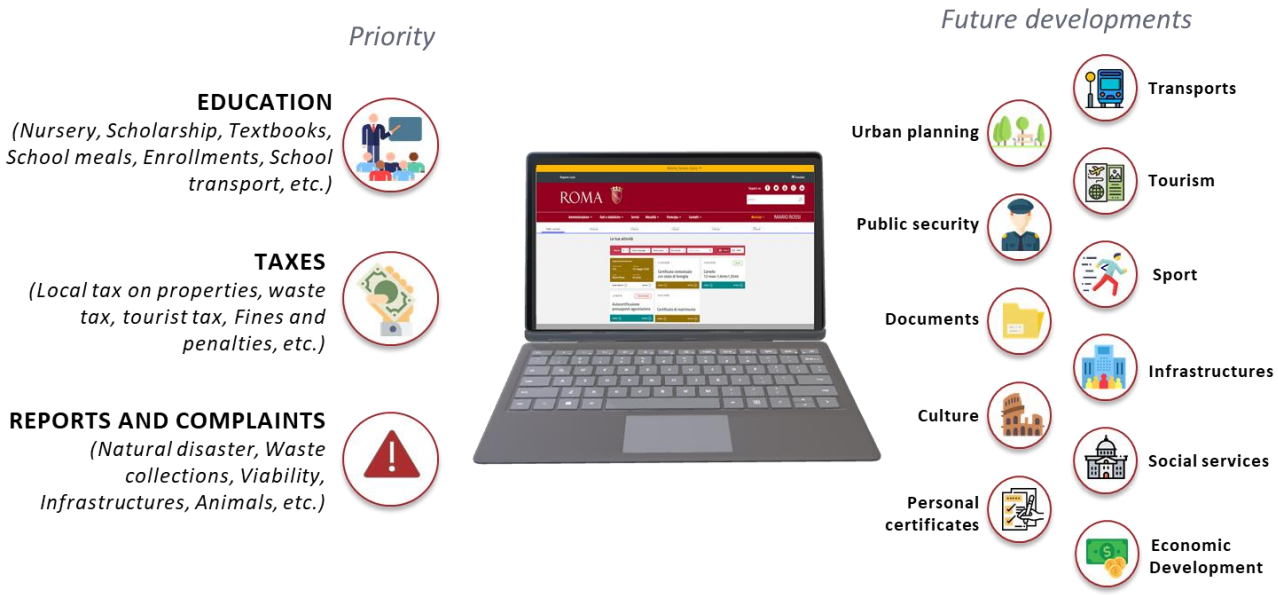

Figure 6.1: Domains for implementation of a Smart City Strategy in Rome (2020)

The RDT at the core of the strategy is the central hub for collecting data, processing data and distributing it to end user applications (Figure 6.2). The platform has following core responsibilities:

- RDT is an IT Data Platform aims to data integration between Administration and external data sources and to improve **data-driven governance policies**.
- RDT offers built-in, ready to use services but also **functions that can be integrated into other applications**.
- RDT supports **ecosystems' growth**.
- RDT is an enabler of **Public Private Partnership models** for data management.

In general, the increasing ability and affordability to collect, process and store increasing amounts of data collected from a multitude of sensing and collection devices in a multitude of use case scenarios allows to process and fuse the data to be applicable to the needs of a wider range of end user groups than is served today by digital administration.

While the scope of the wide-ranging smart city efforts of the city of Rome certainly have a dimension that only metropolitan areas can cope with, the continuing digitization of services and growing availability of data will also compel medium and small sized municipalities to implement smart city applications. For example, our partner city of Larissa – as an example of a medium sized municipality - has recently implemented city wide smart infrastructure projects, and has plans for further applications.

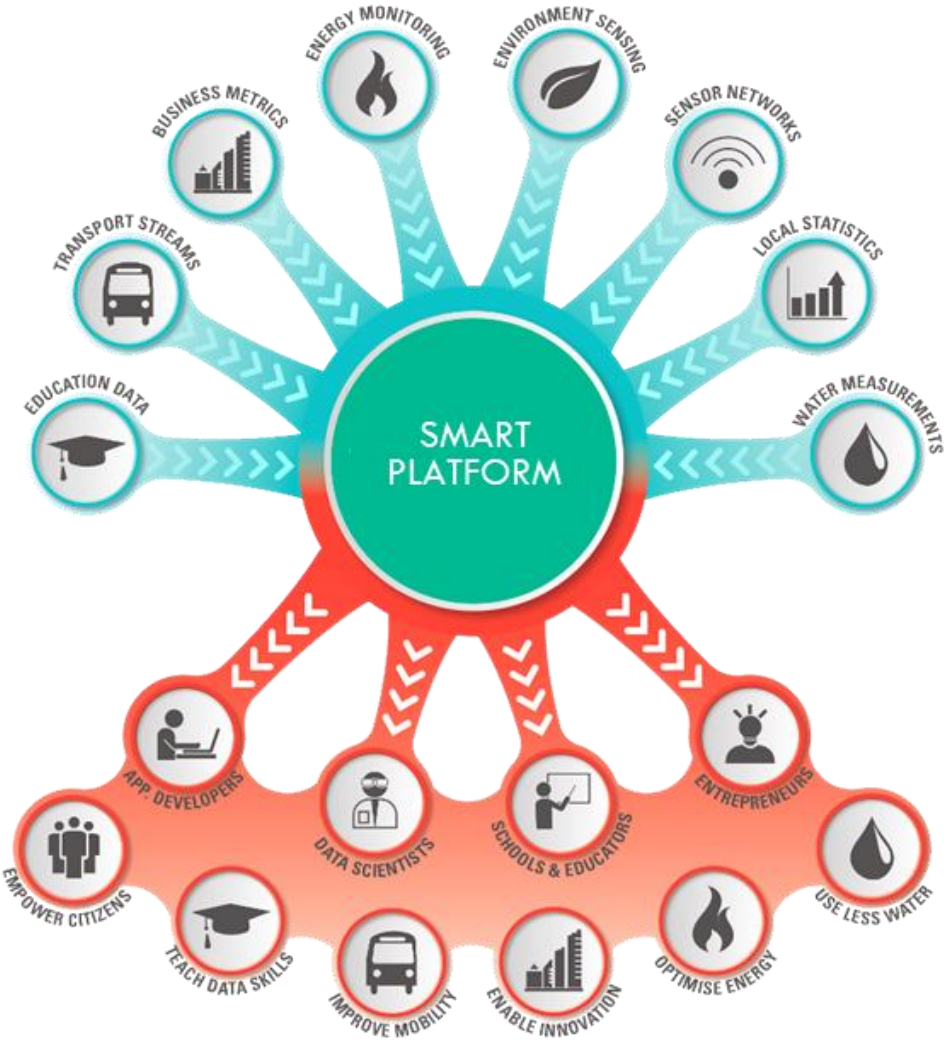

Figure 6.2 The Roma Data Platform

From a security perspective, smart city applications will necessitate a stronger interconnection of enabling technologies like for example IoT, 5G connectivity, AI, smart traffic applications to collect and process relevant data. Furthermore, the volume of data that will be collected will increase significantly, and the data will need to be more personal for many smart city applications to work.

Aside from that, the general service model of data collection, data processing, data storage and data visualization/utilization will follow the same principles as it does today.

Given those circumstances, the CS-AWARE approach is very well suited to deal with the cybersecurity awareness requirements of emerging smart city applications. The identification of assets, dependencies, information flows and business processes and monitoring points – and how those aspects relate to the cybersecurity state of the application – is the first step in any new application that is monitored by CS-AWARE. Due to flexibility that the elicitation of the individual application/service requirements brings, and the way we translate those aspects into monitoring patterns, CS-AWARE is entirely ready for the smart city future!

6.4.2 e-Democracy and e-Governance in the EU due to COVID-19

The COVID-19 pandemic created an increased need for remote working, which in turn demanded for an extensive use of Information and Communications Technology (ICT). For the vast majority of employees this meant that they should be given access to the systems they require for carrying out their everyday tasks. Similarly, Officials had to perform any decision-making processes (e.g. Council Boards) in a fully electronic way. From the citizens' point of view, several services they were used to access in a physical manner would now have to be provided electronically. In order to achieve this state, several technological solutions were employed extensively, one of which being the Virtual Private Network (VPN). This allowed employees to securely connect to their organisation's internal network and carry out their work.

The notion of e-Democracy has been around for quite some time and involves the use of ICT to support the democratic decision-making processes (Macintosh 2004). Another related notion, that of the e-Government, concerns the application of IT for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems between government to citizen (G2C), government-to-business (G2B), government-to-government (G2G), government-to-employees (G2E) as well as back-office processes and interactions within the entire government framework (Saugata, 2007).

For most EU countries, the COVID-19 pandemic triggered a transition to a fuller implementation of both e-Democracy and e-Government. For countries that had a relatively small and/or partial implementation of e-Democracy and/or e-Government, the transition turned out to be quite a violent and fast-paced one. What is more, the cost of this transition is not to be neglected, since a significant investment was made on hardware and/or online services and this equipment is therefore expected to continue being used quite extensively. In addition, the economic impact of the COVID-19 pandemic is expected to force them on budget cut-downs in the near future and hence their only choice may be to continue their operation remotely, via electronic services.

Within this domain, the CS-AWARE approach can be applied productively. As far as Local Public Administrations (LPAs) are concerned, there are cases where a council board concerning a large administrative region has to be held and representatives from smaller LPAs (yet belonging to the same administrative region) have to participate. This is therefore expected to lead to having many more remote users (e.g. via VPN or teleconference software), which are harder to manage and monitor for cybersecurity issues. For instance, the location where each user is connected from may be an initial indicator regarding a potential breach of confidentiality that crosses the country's borders. Another example could be a malicious

participant who is trying to gain access to information and systems they are not supposed to. Given the increased complexity and the large number of users, cybersecurity awareness would be extremely valuable from the IT administrators point of view, as it would give them in real-time the wider picture of what is happening in the information system, they are responsible for.

References

Hibshi, H., Breaux, T. D., Riaz, M., & Williams, L. (2016). A grounded analysis of experts' decision-making during security assessments. *Journal of Cybersecurity*, *2*(2), 147–163.
Macintosh, A. (2004). "Characterizing E-Participation in Policy-Making" (PDF). International Conference on System Sciences. http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan038449.pdf (Accessed 28/08/2020).

Mäkitalo, Å. (2016). On the notion of agency in studies of interaction and learning. *Learning, Culture and Social Interaction*, *10*, 64–67. https://doi.org/10.1016/j.lcsi.2016.07.003

Saugata, B., and Masud, R.R. (2007). *Implementing E-Governance Using OECD Model(Modified) and Gartner Model (Modified) Upon Agriculture of Bangladesh.* IEEE. 1-4244-1551-9/07.