Information & Security

J. Rajamäki
vol. 47, no. 1 (2020): 91-108
https://doi.org/10.11610/isij.4706

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Resilience Management Framework for Critical Information Infrastructure: Designing the Level of Trust that Encourages the Exchange of Health Data

Jyri Rajamäki (✉)

Laurea University of Applied Sciences, Finland, https://www.laurea.fi/en/

ABSTRACT:

This article presents the conceptual resilience governance framework and design aspects for resilient cyber-physical eHealth systems. Our safety and security thinking has been based on the supposition that inside defensive walls we are safe. The focus of our actions has been the control of our own systems, the improvement of the protection and staying inside the protection. However, nobody is able to control complex large integrated cyber-physical systems while, on the other hand, coordination and cooperation are needed. In eHealth, this means that the focus is moved from the control and securing of health information towards utilising of eHealth to promote health. On the other hand, we have an urgent need to complement the existing knowledge-base of safety and risk management by developing frameworks and models enabling network-wide resilience management that strives for maintaining and improving critical functionalities.

ARTICLE INFO:

RECEIVED: 08 MAY 2020
REVISED: 03 JUL 2020
ONLINE: 10 AUG 2020

KEYWORDS:

Resilience management, critical information infrastructure protection, cybersecurity, SHAPES project

1. Introduction

The use of information and communication technology (ICT) in the health and care (H&C) sector has increased due to the potential improvements in effectiveness and efficiency. The target of this design science research (DSR) is to design

✉ E-mail: jyri.rajamaki@laurea.fi

the level of trust that promotes to exchange health data for promoting the health of citizens. Figure 1 presents this study's DSR framework.

The Relevance Cycle of DSR bridges the contextual environment of the research project with the design science activities.[1] This DSR's environment is the eHealth domain, which is considered via the findings of two Horizon 2020 projects (ECHO and SHAPES). The main problem with regard to this DSR: Mental-picture of CS should turn from "threat, crime, attack" to "trust" and willingness to share. *The Rigor Cycle* connects the design science activities with the Knowledge Base of scientific foundations, experience, and expertise that informs the research project.[1] The knowledge base of this study consists of 1) cybersecurity science, 2) concepts of cyber resilience, 3) trust-building in the digital world, and 4) situational awareness in cyber systems. *The* central *Design Cycle* iterates between the core activities of building and evaluating the design artifacts and processes of the research.[1]

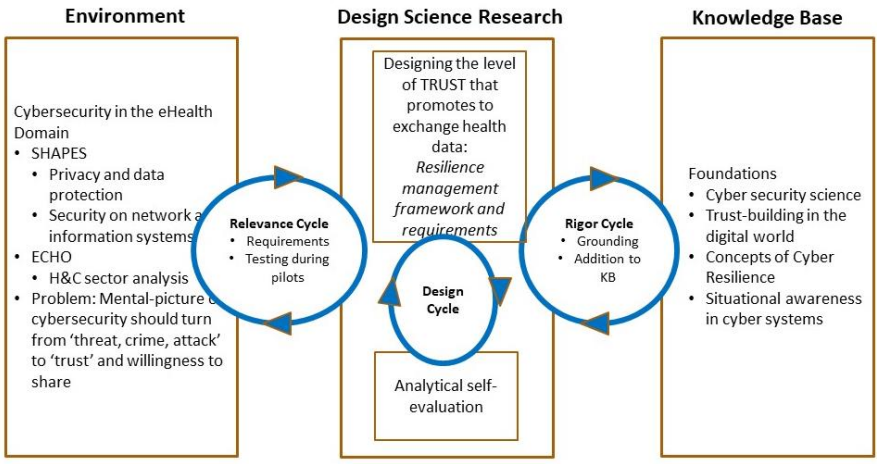

Figure 1: Design Science Research framework of the study (modified from [1]).

The rest of the paper is structured according to Figure 1: Section 2 presents the environment of the study; Section 3 deals with the knowledge base; Section 4 focuses on the designing process of the proposed resilience management framework; Section 5 discusses the results.

2. Method Cybersecurity in the eHealth Domain

2.1. The SHAPES Project

Digital transformation and ecosystem thinking steer the Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES) project[2] supports the well-being of the elderly at home. The SHAPES project is an ambitious endeavour that gathers stakeholders from across Europe to create, deploy and pilot at large-scale an EU-standardized open platform incorporating and inte-

grating a broad range of solutions, including technological, organizational, clinical, educational and societal, to enable the aging population of Europe to remain healthy, active and productive, as well as to maintain a high quality of life and sense of wellbeing for the longest time possible.

In the nursing and caring literature, technology as a concept has three implications:[3] 1) technology is devices and products, including ICT and advanced, simple and assistive technology; 2) technology refers to a process consisting of methods for helping people; 3) technology as a service indicates the production of care by technology. From the perspective of caring science, this outlines technology as products and devices used in care, whereas technology as a process refers to all methods helping people in caring relationships and promoting good in health, sickness, and suffering. Technology as a process is essentially interactive. Nurses act as interpreters between patients and technology. Finally, technology as a service means producing care by using technology and its applications in the act of caring. When the act of caring comes true in the ethical and caring way, the human dignity and human rights as well as human good of the patient's realized and the potential harms will be prevented.

2.1.1. Privacy and data protection

Data Protection refers to legislation that is intended to 1) protect the right to privacy of individuals (all of us), and 2) ensure that Personal Data is used appropriately by organizations that may have it (Data Controllers). Personal data is any information that can be used to identify a natural person (Data Subject), such as name, date of birth, address, phone number, email address, membership number, IP address, photographs, etc. Some categories of information are defined as 'special categories of personal data' (e.g., religion, ethnicity, sexual orientation, trade union membership, medical information) and they require more stringent measures of protection. Also, criminal data and children's data need additional protection. The EU General Data Protection Regulation (GDPR) is a mandatory requirement for eHealth services. Besides this, one of the key messages in the health care market is that when ensuring that digital solutions are safe and users can trust that their data is secured and used in an ethical way, this will be a huge advantage.

Figure 2 describes the different elements that link to the usage of personal data in the SHAPES project. Personal data is defined widely in the GDPR, with the aim to get all such data under the scope of legislation that can be linked to an individual person. Identifying personal data is the first task when we are planning the data usage in SHAPES. The diagram in the middle of the picture illustrates the different ways the data can be used. It is good to notice that the list is not comprehensive; those are examples of the most commonly used processing methods. The boxes on the right side of the picture describe the roles that, e.g., a company can have when processing personal data. The arrows give an example of how personal data can be transferred or disclosed from one party to another. 'Transferring' means that the data can be used only according to the given instructions from the controller, and 'the disclosure' means the data will

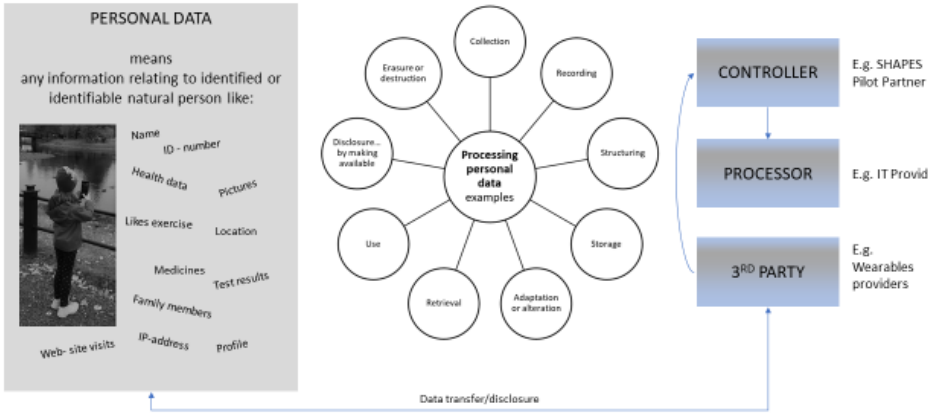

Figure 2: Processing of personal data in SHAPES.[4]

be given to a third party who will, after the disclosure, work as a controller for such data. When personal data is processed as part of SHAPES, all aspects described in the picture needs to be analysed and documented.

2.1.2. Security on Network and Information Systems (NIS) Directive

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 ('NIS Directive') is a piece of EU-wide legislation on cybersecurity providing some minimum standards. It applies to the Member States and two groups of organizations: operators of essential services (OES) and relevant digital service providers (RDSPs). OES include critical industries such as energy, transport, healthcare, and financing. RDSPs offer one or more of the following services: 1) an online marketplace; 2) an online search engine, or 3) a cloud computing service.

Critical infrastructures are not secure from cybersecurity threats, and citizens cannot be sure of the security of the systems they use daily. The overall risk (operational, economic, reputational) can be high (medium likelihood and high impacts), and possible risk indicators are: 1) lack of information necessary to assess the security of network and information systems, including documented security policies; and 2) lack of evidence of the effective implementation of security policies.

The objective of the NIS Directive to drive different companies to use IT security solutions and establish practices to protect IT networks and data – both their own and those of third parties. The European Commission, therefore, wants to stem the phenomenon of cybercrime that has become popular in recent years: more and more, companies are being hacked, resulting in the theft of data. The consequences of a successful attack are often heavy, both in terms of economic and reputational losses.

Preventing the risk with mitigation actions, it is possible to commit for the following opportunities of improvement:

1. Technical requirements:

– Understanding one's own resources and having a tool for identifying unknown devices
– A vulnerability management program
– Advanced systems for threat detection, including detection, identification and reporting capabilities
– Effective mechanisms for reporting incidents, including systems to record and report incidents within 72 hours of detection to CSIRTs
– Effective incident management
– Response and recovery plans

2. Organizational requirements:

– An organizational approach to risk management
– Adequate management policies and processes to govern the approach to security of networks and information systems
– Understanding and management of security risks throughout the production chain
– Adequate staff training and awareness in the field of security of networks and information systems
– A CSIRTs network established and composed of representatives of the Member States' CSIRTs and CERT-EU
– Designation of each Member State to have one or more competent national authorities on the security of network and information, covering at least the sectors of OES and DSP
– A cooperation group established in line with article 11
– When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall consider at least the cross-sectoral factors stated in Article 16
– Article 14 security requirements and incident notification for OES
– Article 16 security requirements and incident notification for DSP

Application in the healthcare sector

The NIS Directive imposes different obligations on operators of essential services, and healthcare entities will almost always fall under the definition of operator of essential services (Art. 4, 4, Art. 5, 2 and Annex II Directive (EU) 2016/1148) and thus need to comply with its provisions. 'OES' will need to prevent and minimize the impact of disruptions affecting the security of their systems and take technical and organizational measures to reduce the risk posed to the security of their network and information systems. They also need to notify the competent authority of every incident that has a significant disruptive effect on the service.[5]

Applications within digital services

Online marketplaces are digital services that allow individuals or traders to carry out sales or service contracts with traders, either on their own websites or by means of providing services to traders' websites. Online retailers that sell directly to individuals on their own behalf are not covered.

Cloud services are digital services that enable access to a scalable and elastic pool of shareable computing resources. This can include common cloud models like "platform as a service" (PaaS) and "infrastructure as a service" (IaaS). If you provide "software as a service" (SaaS), you are also covered to the extent that your service is scalable and elastic.

The EU Commission has also published an implementing act, Regulation 2018/151. It is specifically concerned with digital service providers, including their security requirements and incident reporting thresholds.

NIS Directive and SHAPES

As discussed above, the NIS Directive applies to SHAPES: the SHAPES platform can be considered to be RDSP, and SHAPES service providers can be considered to be OES. Because the NIS Directive is a minimum directive, the legislations of member states can be stricter than the minimum requirements provided by the NIS Directive. The legislation of the Member State in question with which the directive has been brought into effect has to be checked before carrying out the SHAPES pilots. Then one must act in accordance with this national legislation.

2.2. Cybersecurity Research in the H&C Domain in the ECHO Project

ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) is one of the four pilot projects under the H2020 pro-gram with the objective of connecting and sharing knowledge across multiple domains to develop a common cybersecurity strategy for Europe. The ECHO Multi-Sector Assessment Framework provides a structured method for multi-dimensional analysis of security disciplines (e.g., cryptography, network security, application security, IoT/cloud security, etc.); sector-specific use cases (e.g., analysis of sector-specific needs and challenges); transversal cybersecurity needs analysis (e.g., common cyber-security needs such as policies, regulations, and skills frameworks); and inter-sector technology and dependency analysis (e.g., identification of common technology roadmaps solving inter-sector technology challenges). One of the sectors analyzed in the ECHO Project is H&C. Table 1 lists the relevant deliverables published/submitted so far, and Table 2 presents the sub-jects of the H&C related analyses in ECHO Deliverables.

3. Knowledge Base

As Hevner and Chatterjee [1] state design science draws from a vast knowledge base of scientific theories and engineering methods that provides the foundations for rigorous DSR. This section defines the state of the art in the application do-main of the research.

Table 1. ECHO Deliverables dealing with H&C sector.

Publication/Deliverable	version	date
ECHO D2.1 Sector scenarios and use case analysis	1.0	31/10/2019
ECHO D2.2 ECHO multi-sector assessment framework	1.0.15	31/10/2019
ECHO D2.4 Inter-sector technology challenges and opportunities	1.0	31/10/2019
ECHO D2.5 Multi-sector requirements definition and demonstration cases	1.0	31/01/2020

Table 2. ECHO Project's H&C sector cybersecurity-related published analyses.

Aim of analysis	Deliverable	Section
Known cyber-attacks in the H&C domain	D2.1	4.1.1
Cybersecurity threat trends in the H&C domain	D2.1	4.1.2
Scope and context of an H&C scenario	D2.1	4.1.3
Description of a Health Care scenario • Storyline HC01 "Social engineering attacks on hospital staff" • Storyline HC02 "Tampering with medical devices" • Storyline HC03 "Theft or loss of hospital equipment or data" • Storyline HC04 "Malware attacks on hospital information systems"	D2.1	4.1.4
Study of inter-sector cybersecurity dependencies. Telecommunication and H&C sectors	D2.1	5.2
Modelling and analysis of the use cases of the H&C scenario	D2.1	6.3
Analysis of existing cybersecurity framework adoption in the H&C domain. • NIST Cyber Security Framework • HITRUST Common Security Framework • CIS Critical Security Controls • ISO 27000 • COBIT • ECHO healthcare scenarios: weaknesses and potential mitigation actions	D2.2	3.2

• Conclusions		
Inter-sector and transversal aspects. H&C		
Analysis of selected scenarios and use-cases per sector – technological context. Analysis of selected sectors: H&C	D2.2 D2.4	3.6.3 3.1.1
Identified common technological opportunities/ countermeasures to be targeted: H&C	D2.4	3.3.1
Sector-specific issues and solutions – technological context: H&C	D2.4	3.4.1
Inter-sector cybersecurity challenges, opportunities, and dependencies. Cybersecurity challenges and opportunities in the H&C sector	D2.5	3.3.1
Analysis of inter-sector cybersecurity dependencies. Dependencies between Healthcare, Telecommunication, Navigation and Big Data	D2.5	Table 6
Multi-sector analysis. Healthcare sector analysis	D2.5	4.2.2.3

3.1. Cyber Security Science

The aim of cybersecurity is to make cyberspace safe from damage or threat. Figure 3 shows three perspectives of cyberspace: (1) a data or information perspective that comes from the information theory space; (2) a technology perspective that includes the hardware, silicon, and wires, as well as software, operating systems, and network protocols; and (3) a human perspective that acknowledges that the human is as responsible for the dynamics of the system as the data and the technology are.[6]

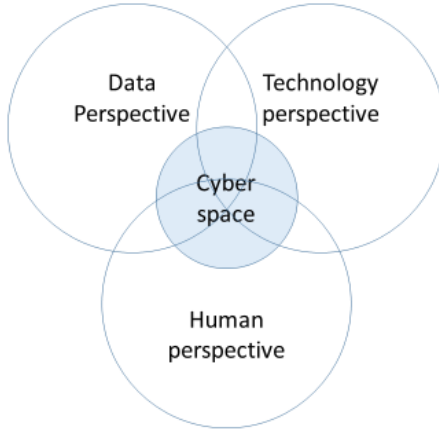

Figure 3: Cyberspace at the overlap of data, technology and human.[6]

3.2. Building Cyber-Trust

The purpose, with regard to security, is to know what is going on and what will happen in the network(s), and to be aware of the current level of security in the network(s), how to design or build-in security and resilience to a networked environment, and to define trade-offs for security and privacy levels versus system's usability.[7] The overall aim is to mitigate cybersecurity risks, which in turn sup-ports the business continuity and operations of the whole society.[7]

Figure 4: Themes of Trust-building (adapted from [7]).

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cybersecurity should be seen as a key enabler for the development and maintenance of trust in the digital world. Cybersecurity has the following four themes:[7] (1) security technology, (2) situational awareness, (3) security management, and (4) resilience, as shown in Figure 4. Situational awareness is needed for having a correct understanding of security incidents, network traffic, and other important aspects that affect security; and security technologies are needed for protection.[7] Human aspects have to rule in via security management. Consequently, resilient systems and infrastructures have the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events.

3.3. Fundamental Concepts of Cyber Resilience

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructure lacks the same degree of resilience, typically losing essential functionality following adverse events.[8] Without proper protection and development with cybersecurity in mind, modern society relying on critical infrastructures would be extremely vulnerable to accidental and malicious cyber threats. Resilient systems are able to minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events.[8]

The Network-Centric Warfare (NCW) doctrine [9] identifies four domains that create shared situational awareness and inform decentralized decision-making:

1. Physical: Physical resources and the capabilities and the design of those resources;
2. Information: Information and information development about the physical domain;
3. Cognitive: Use of the information and physical domains to make decisions; and
4. Social nexus: Organization structure and communication for making cognitive decisions.

The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient: [10]

1. Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack).
2. Absorb: Maintain the most critical asset function and service availability while repelling or isolating the disruption.
3. Recover: Restore all asset function and service availability to their pre-event functionality.
4. Adapt: Using knowledge from the event, alter protocol, a configuration of the system, personnel training, or other aspects to become more resilient.

Linkov et al.[11] combined the event management cycles and NCW domains to create resilience metrics for cyber systems. The fundamental concepts of cyber resilience applied in this DSR are based on the book "Cyber Resilience of Systems and Networks," Springer 2018.[12] The process of building resilience is a collective action of public and private stakeholders responding to infrastructure disrup-tions.[13]

3.4. Situational Awareness in Cyber-Systems

As Figure 4 shows, situational awareness (SA) is the main prerequisite of cybersecurity and resilience. Without SA, it is impossible to systematically prevent, identify, and protect the system from cyber incidents and if a cyber-attack happens, to recover from the attack.[7] SA involves being aware of what is happening around your system to understand how information, events, and how your own actions affect the goals and objectives, both now and in the near future. It also enables selection of effective and efficient countermeasures, and thus, to protect the system from varying threats and attacks.

Situational awareness is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resilience focuses. The most important enablers of SA are observations, analysis, visualization, governmental cyber-policy, and national and international cooperation. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, are needed. This requires information exchange between

different stakeholders. And always, when dealing with information exchange, the main question is "trust".

Cyber situational awareness high-level architecture (see Figure 5) includes the data fusion engine, information interfaces, and the HMI providing an effective visualization layer.[14] These functionalities should be as automatic as possible without human interaction. However, there should be an operator for controlling the sensors and data fusion algorithms and inputting information to the system.

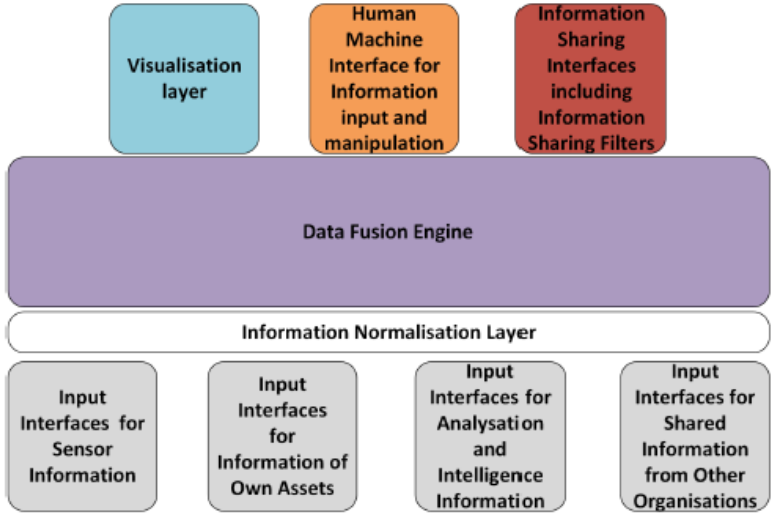

Figure 5: High level cyber situational awareness architecture.[14]

The cognitive SA system for supporting decision-making needs several input and output interfaces: [14]

1. Sensor information interfaces. The system implements interfaces for the input of cybersecurity sensor information.

2. Interfaces for status information. The system implements interfaces for input-ting the status information of all the known cyber entities. Information on systems, devices, and sensors with their status and configuration information, but also the spare parts of physical devices are relevant information for a cybersecurity SA system. Also, information about the status of saved data and the status of information flows should be reported. Some of that information can be automatically generated using data interfaces and some should be user-generated by using HMI.

3. Interfaces for analysis information. The system implements interfaces for in-formation based on the analysis. That kind of information includes analysed impact assessment information, Indicator of Compromise (IOC) information, and early-warning information from open-source intelligence using, e.g., social

media or CERT bulletins. Further, required policies and objectives should be input to the system.

4. Interfaces for information exchange. The system implements interfaces for cybersecurity information exchange with trusted companions.

5. HMI. The system implements HMI for effective visualization of the current status of the cyber domain under control and for the input of information that cannot be entered automatically. HMI is also used for controlling the data fusion process. HMI should implement different visualizations for different levels of users: e.g. technical user who requires detailed technical information, whereas a decision-maker needs totally different visualization. HMI also implements filters for data allowed for different users.

4. Resilience Management Framework and Requirements

4.1. Rationale behind eHealth Cybersecurity and Resilience Requirements

The overall goal of cybersecurity is that all systems and infrastructures are resilient. An eHealth platform is a cyber-system that has human, technology, and data domains (see Fig. 3).

One can think of a cyber-system as consisting of two sub-systems: the proper resilient operating system and the (*cognitive*) situational awareness system that both have human (*social*), technological (*physical*), and data-based (*information*) domains. Figure 6 shows this concept. *Security management, security technologies,* and *security information* connect these sub-systems. However, security information is mostly created or transferred from the operational system to the SA system via security technologies.

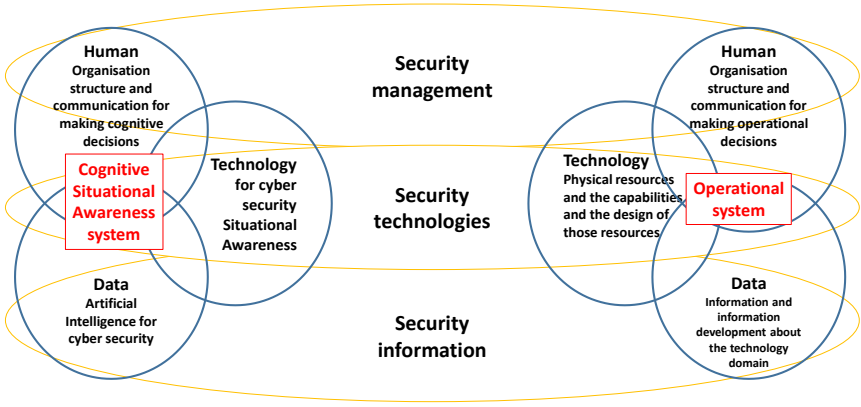

Figure 6: Resilient Cyber-system as a combination of Operational system and Cognitive SA system.

4.1.1. Security management and governance

Security policy is currently the main element used to communicate secure work practices to employees and ICT stakeholders. It is a declaration of the significance of security in the business of the organization in question. Additionally, the security policy defines the organization's policies and practices for personnel collaboration. However, people still often fail to comply with security policies, exposing the organization to various risks. One challenge is to promote methods and techniques that can support the development of comprehensible security policies in the emerging ICT paradigms, e.g., cloud computing and multiple devices. [7] Developing policies that can defeat the main reasons driving noncompliance, such as a habit, is challenging.

An information security management system (ISMS) focuses on the continuous management and operation of a system by the documented and systematic establishment of the procedures and processes to achieve confidentiality, integrity, and availability of the organization's information assets that do the preservation. ISMS provides controls to protect organizations' most fundamental asset, information. Many organizations apply audits and certification for their ISMS to convince their stakeholders that the security of the organization is properly managed and meets regulatory security requirements. An information security audit is an audit on the level of information security in an organization. Security aware customers may require ISMS certification before a business relationship is established. Unfortunately, ISMS standards are not perfect and they possess potential problems. Usually, guidelines are developed using generic or universal models that may not be applicable for all organizations. Guidelines based on common, traditional practices take into consideration differences of the organizations and organization-specific security requirements.

In Figure 6, *security management* covers the human and organizational aspects of cybersecurity. Its focus areas include security policy development and implementation, risk management and information security investment, incentives, and trade-offs. Security management also integrates the social layer's operational and cognitive aspects; all technical and organizational components should learn from prior events and incidents.

4.1.2. Security management and governance

Security technologies include all technical means towards cybersecurity, such as secure system architectures, protocols, and implementation, as well as tools and platforms for secure system development and deployment. Security technologies are needed for fulfilling the recognized security requirements, and for building resilient infrastructures and systems with dependable hardware and software that can also meet future security challenges. [7]

Security technologies enable the technical protection of infrastructures, platforms, devices, services, and data. The technical protection starts with secure user identification and authorization that are necessary features in most secure infrastructures, platforms, devices, and services. Fortunately, well-known technologies exist for their implementation. Typically, processes and data objects

are associated with an owner, represented in the computer system by a user account, who sets the access rights for others. A global trend is to increase the use of cloud service technology when providing critical services. Data go into a cloud and will not come back to end-users' devices. Also, government data has already gone to a cloud, and in the future more and more government data will migrate to cloud servers and services. Partnerships between cloud service providers and security solution providers are becoming more common. We will see the emergence of cloud service-specific-solution providers as well. Identity management and encryption will be the most important cloud security services to be offered. These services will be eventually offered for small to medium-sized businesses as well. We will also see the emergence of cloud security standards. Challenges are that quite often cloud service providers believe that security is just an end-user issue and firewall means security. Therefore, currently, we do not have proper cloud security standards and we lack awareness of a true understanding of comprehensive cloud security.[7]

Security technologies are needed also then if something has happened. For example, forensics can lead to the sources of the attack/mistake and provide information for legal and other ramifications of the issue. Forensics also facilitates the analysis of the causes of the incident, which in turn, makes it possible to learn and avoid similar attacks in the future.

In Figure 6, *security technologies* include all technical means towards cybersecurity, such as secure system architectures, protocols, and implementation, as well as tools and platforms for secure system development and deployment. Technologies that create or transfer *security information* from the operational system to the SA system include sensors that collect the first level of data. Commonly, host- and network-based tools generate logs that are used for SA. Firewalls, system event logs, antivirus software, packet captures, net flow collectors, and intrusion detection systems are examples of common cyberspace sensors.[6] Level-two technologies generate information from the data to determine a current situation. Generally, level-two technologies require the bringing together of data and performing some level of analytics. The simplest form is signature-based tools such as antivirus and intrusion detection systems. These systems have encapsulated previous knowledge of detected attacks into signatures that detect and alert when attacks are detected in operational systems. More advanced systems such as security information and event managers (SIEMs) provide infrastructure to bring together datasets from multiple sensors for performing correlations. Also, vulnerability analysis to determine how many unpatched vulnerabilities exist in a system is also a form of level-two technology.[6] The third and final level is hard to achieve and only a few examples of effective tools exist. Cyber-threat intelligence provides information on active threat actor methods, techniques, and targets providing some level of predictive information to enable taking pre-emptive security measures.[6] Artificial intelligence for cybersecurity develops with high speed and offers new possibilities for better SA.

4.1.3. Cognitive situational awareness and resilience management

Increasingly interconnected social, technical, and economic networks create large complex systems, and risk assessment of many individual components becomes cost and time prohibitive, or even impossible.[8] No one can control the whole system of infrastructures, and our outlook should move to co-ordination and co-operation. The uncertainties associated with the vulnerabilities of these systems challenge our ability to understand and manage them. Risk assessment and risk management are no longer sufficient in the modern cyber-physical world, which has unforeseeable and non-calculable stress situations. To address these challenges, a risk assessment should be used whenever possible to help prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events do occur.[8]

The cognitive situational awareness system in Figure 6 utilizes the information from the operational system to make decisions that aim towards better resilience.

4.2. Resilience Governance Framework and Requirements

Figure 7 presents the conceptual resilience governance framework for a resilient eHealth cyber-system. From that framework, the following five cybersecurity and resilience requirement can be derived for the platform:

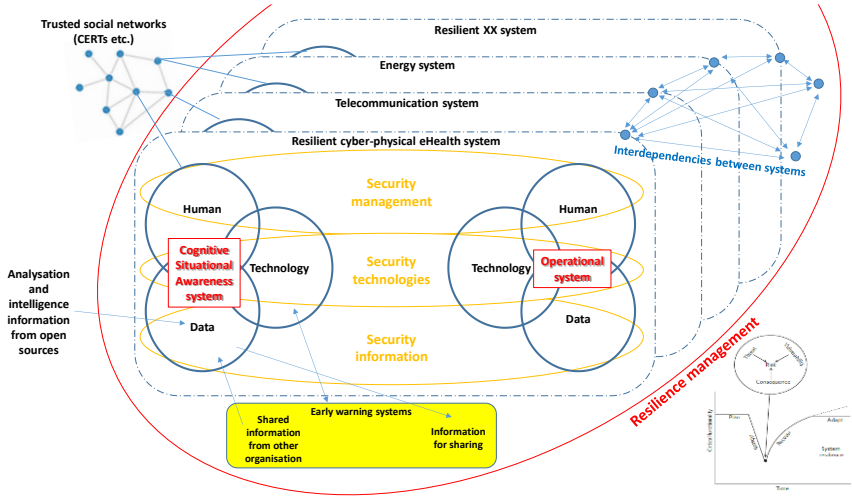

Figure 7: Conceptual resilience governance framework for eHealth CPSs.

1. Design and implement a security management plan
   - Carry out cyber risk management

- Identify and coordinate with external entities that may influence or be influenced by internal cyber-attacks (establish a point of contact)
- Educate and train employees about cybersecurity and the organization's security management plan
- Delegate all assets and services to specific employees
- Prepare security communications

2. Establish a cyber-aware culture
   - Employ all appropriate *security technologies*
   - Implement controls/sensors for critical assets
   - Implement controls/sensors for critical services
   - Assess network structure and interconnection to system components and the environment
   - Implement redundancy of critical physical infrastructure
   - Assess the redundancy of data physically or logically separated from the network
3. Ensure the adequacy and quality of *security information* (suitability for AI)
   - Categorize assets and services based on the sensitivity
   - Document certifications, qualifications and pedigree of critical hardware and/or software providers
   - Prepare plans for storage and containment of classified or sensitive information
   - Identify internal system dependencies
4. Make sure that *situational awareness* is always up to date (cognitive domain)
   - Anticipate and plan for system states and events
   - Understand the performance trade-offs of organizational goals
   - Set up scenario-based cyber war-gaming
   - Utilize applicable plans for system state when available
   - Utilize artificial intelligence or prepare to utilize it for responding to threats with greater confidence and speed
5. Design and implement *a resilience management plan* that covers all four event management cycles (plan/prepare, absorb, recovery, adapt) and interdependencies with other systems
   - Consider how all previous requirements can be utilized throughout the four event-management cycles
   - Identify external system dependencies (i.e., telecommunication, electricity, built environment), and plan the coordination framework with these systems (you have no control for these systems)
   - Educate and train employees about resilience and the organization's resilience plan

5. Discussion

From a citizens' point of view, eHealth is wholeness in which sectors of information security (availability/confidentiality/integrity) hold true. Present procedures emphasize confidentiality at the expense of integrity and availability,[15] and regulations/instructions are used as an excuse not to change even vital

information. The mental-picture of cybersecurity should turn from 'threat, crime, at-tack' to 'trust'. Creating confidence in a safe digital future is truly needed in the integration of digital and physical worlds, leading to a digital revolution. Digitalization and new, better services require cooperation. Safety-and-security thinking has been based on the supposition that we are safe and we are able to prevent 'bad touch', and the focus of actions has been the control of our own systems, improvement of protection, and staying inside that protection. However, nobody is able to control large, complex, integrated cyber-physical systems, but on the other hand, coordination and cooperation are needed, because the process of building resilience is a collective action of public and private stakeholders responding to infrastructure disruptions.[13] In the H&C sector, this means that the focus is moved from the control and securing of health information towards utilising of eHealth to promote health. We have an urgent need to complement the existing knowledge-base of security and risk management by developing frame-works and models enabling network-wide resilience management that strives for maintaining and improving critical functionalities.

In this paper, the cybersecurity and resilience aspects of the SHAPES Integrated Care Platform have been discussed. On the basis of these contents and arguments, five high-level cybersecurity and resilience requirements have been defined. The purpose of these requirements is to ensure that SHAPES becomes a positive innovation for various end-users, service providers, and society. These cybersecurity and resilience requirements are intended to launch a more detailed discussion of the ethics of SHAPES with its developers during the first 1.5 years of the project. Based on those requirements, technical notes are also to be produced, if necessary, to support the implementation of the requirements as features of the SHAPES Technical Platform and of the SHAPES Marketplace and Ecosystem.

Acknowledgements

This work was supported by the SHAPES project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 857159.

References

1 Alan Hevner and Samir Chatterjee, *Design Research in Information Systems: Theory and Practice* (New York: Springer Science and Business Media, 2010).

2 European Commission, "Smart and Healthy Ageing through People Engaging in Supportive Systems," 2019, available at: https://cordis.europa.eu/project/id/857159.

3 Eila-Sisko Korhonen, Tina Nordman, and Katie Eriksson, "Technology and Its Ethics in Nursing and Caring Journals: An Integrative Literature Review," *Nursing Ethics* 22, no. 5 (2015): 561-576.

4 N. Alapuranen, "SHAPES Privacy and Data Protection," in *D8.4 – SHAPES Ethical Framework* (Brussels, European Commission, 2020), 48-59.

5 SecureHospitals, available at: https://www.securehospitals.eu/nis-directive/.

[6] Thomas Edgar and David Manz, *Research Methods for Cyber Security* (Cambridge: Syngress, 2017).

[7] DIMECC, "The Finnish Cyber Trust Program 2015–2017," Helsinki: DIMECC, 2017.

[8] Igor Linkov, Todd Bridges, Felix Creutzig, Jennifer Decker, Cate Fox-Lent, Wolfgang Kröger, James Lambert, Anders Levermann, Benoit Montreuil, Jatin Nathwani, Raymond Nyer, Ortwin Renn, Benjamin Scharte, Alexander Scheffler, Miranda Schreurs, and Thomas Clemen, "Changing the Resilience Paradigm," *Nature Climate Change* 4, no. 6 (2014): 407-409.

[9] David Alberts, "Information Age Transformation, Getting to a 21st Century Military. DOD Command and Control Research Program," 2002.

[10] National Academy of Sciences, "Disaster Resilience: A National Imperative," 2012.

[11] Igor Linkov, Daniel Eisenberg, Kenton Plourde, Thomas P Seager, Julia Allen, and Alexander Kott, "Resilience Metrics for Cyber Systems," *Environment Systems & Decisions* 33, no. 4 (2013): 471–476, https://doi.org/10.1007/s10669-013-9485-y.

[12] Alexander Kott and Igor Linkov, *Cyber Resilience of Systems and Networks. Risk, System and Decisions* (Cham: Springer, 2019).

[13] Hans Heinimann and Kirk Hatfield, "Infrastructure Resilience Assessment, Management and Governance – State and Perspectives," in I. Linkov, J.M. Palma-Oliveira (eds.), *Resilience and Risk* (NATO Science for Peace and Security Series C: Environmental Security, Cham, Springer, 2017), 147-187.

[14] Tero Kokkonen, "Anomaly-Based Online Intrusion Detection System as a Senor for Cyber Security Situational Awareness System," *Jyväskylä studies in computing* 251, University of Jyväskylä, 2016.

[15] Jyri Rajamäki and Rauno Pirinen, "Towards the cyber security paradigm of eHealth: Resilience and design aspects," in Klimis Ntalianis (ed.) *AIP Conference Proceedings Vol. 1836, Applied Mathematics and Computer Science: Proceedings of the 1st International Conference on Applied Mathematics and Computer Science*, Melville, AIP Publishing, 2017.

About the Author

Jyri Rajamäki is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology and a PhD in mathematical information technology from University of Jyväskylä.