Towards the cyber security paradigm of ehealth: Resilience and design aspects

Cite as: AIP Conference Proceedings **1836**, 020029 (2017); https://doi.org/10.1063/1.4981969
Published Online: 05 June 2017

Jyri Rajamäki, and Rauno Pirinen

Towards the Cyber Security Paradigm of eHealth: Resilience and Design Aspects

Jyri Rajamäki[1, 2, a)] and Rauno Pirinen[1, 3, b)]

[1]*Research, Development and Innovations, Laurea University of Applied Sciences, Espoo, Finland*
[2]*Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland*
[3]*Facalty of Management, National Defence University, Helsinki, Finland*

[a)]Corresponding author: jyri.rajamaki@laurea.fi
[b)]rauno.pirinen@laurea.fi

Abstract. Digital technologies have significantly changed the role of healthcare clients in seeking and receiving medical help, as well as brought up more cooperative policy issues in healthcare cross-border services. Citizens continue to take a more co-creative role in decisions about their own healthcare, and new technologies can enable and facilitate this emergent trend. In this study, healthcare services have been intended as a critical societal sector and therefore healthcare systems are focused on as critical infrastructures that ought to be protected from all types of fears, including cyber security threats and attacks. Despite continual progress in the systemic risk management of cyber domain, it is clear that anticipation and prevention of all possible types of attack and malfunction are not achievable for current or future cyber infrastructures. This study focuses on the investigation of a cyber security paradigm, adaptive systems and sense of resilience in a healthcare critical information infrastructure.

INTRODUCTION

The intent of this study is that digital healthcare services, later eHealth, have been recognized as a critical societal sector and therefore, eHealth systems are considered here as an instance of critical infrastructures that should be protected from all types of threats, including such as cyber security attacks and malfunctions. In the environment of study, the cyber security paradigm of eHealth is understood as one of the critical entities for the nation and the wellbeing of citizens. One fundamental element of this study is that eHealth security challenges are equal to all critical information infrastructure protection subjects, the main complication of which is the lack of adaptive systems and resilience, typically losing essential functionality in practice.

In this study, the term "resilience" is approached as manners to enhance the capability on all levels of activities to create information processes that are robust yet flexible, to monitor and revise risks, and to use resources proactively in the face of disruptions or pressures of ongoing activities such as eHealth service, learning frames, control, production, trade or engineering. In our cyber view, resilience can be seen as an ability to recover from or build new position to misfortune or adaption of necessary adaptive change; resilience can also be approached by way of four abilities: 1) to plan and prepare; 2) absorb disturbance; 3) recover from; and 4) adapt to known or unknown threats. Then, in this view as cyber security paradigm of eHealth, the sense of "resilience" focuses on the ability of a system, community or society exposed to security and safety related threats to resist, absorb, accommodate to and recover from the effects of a threat in a timely and efficient manner, including through the adaption, preservation and restoration of its essential basic structures and functions.

Applied Mathematics and Computer Science
AIP Conf. Proc. 1836, 020029-1–020029-9; doi: 10.1063/1.4981969
Published by AIP Publishing. 978-0-7354-1506-5/$30.00

LITERATURE REVIEW

Security and Privacy Aspects in eHealth

The digital security of information is traditionally expressed in terms of maintaining three characteristics of the information: confidentiality, integrity and availability. In addressing the provision of data security services for information assets, it is necessary to consider the state of the information: is it in storage, in transmission, or in use as being processed. When considering possible aspects to secure digital information, three classes occur: technological solutions; policy-regulation; and practices related to information management; and the frames of education and situational awareness as views of all stakeholders in the security implications of potential activities. The three characteristics of information, the three states of information and three classes of security aspects form the basis of an information security-resilience frame exists, confer [1] and our furthered Figure 1.

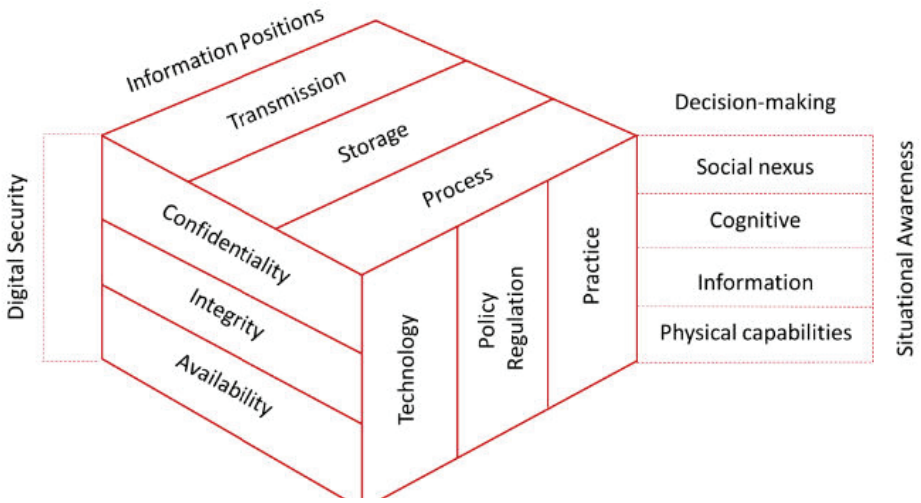

FIGURE 1. Security Aspects for Information Dimensions (modified from [1])

Digital security is generally understood as a 'weakest link' problem, so the system cannot be considered secure unless all aspects are dealt with adequately, and with regard to eHealth, many people consider this unlikely to be achieved, hence, the continuing concerns over information privacy [2]. On the other hand, others consider eHealth systems an opportunity to achieve better security and privacy protection than what is available in paper-based systems through additional security functionalities: user authentications and authorizations, the retention of back-up files, user defined storage and retrievals and accountability measures, monitoring and logging access to records, and establishing audit trails and other mechanisms to enable information accountability [2]. However, these require a more comprehensive approach than an attempt to add on technological security measures to an incompletely specified eHealth system.

Current Cyber Security Challenges in eHealth

In 2015, The European Union Agency for Network and Information Security (ENISA) published their study "Security and Resilience in eHealth" [3] that focus on eHealth information systems and infrastructures as well as on the relevant assets that are considered critical both for the society and the relevant stakeholder groups. This study can be seen as a description of the state of the art how EU member states perceive cyber security in their health systems, which are the specific approaches they follow, and which are the measures they take to protect these systems.

According to the ENISA, the most important cyber security challenges in eHealth infrastructures and systems are: 1) systems availability; 2) lack of interoperability; 3) access control and authentication; 4) data integrity; 5) network security; 6) security expertise and awareness; 7) data loss; 8) standardization, compliance and trust; 9) cross-border incidents; and 10) incidents management:

Systems Availability

Systems availability is the basic feature for achieving continuity of eHealth [3]. It is about continuous accessibility of critical health information by authorized professionals in order to ensure the best healthcare services. Systems availability may relate to physical systems e.g., networks, storage or the maturity of business continuity infrastructure, process in place and integration. The more digitized the health sector being, the more the health services are affected by interruptions in eHealth infrastructures, e.g., if documentation, imaging, laboratory systems and client administration systems are digitized, then network and information system availability is critical.

A violation of processes protocols may lead to the interruption of services, e.g., an operator might cause an interruption by proceeding to an update without following the protocol. In this case, the impact on the continuity of services can be really high. Another parameter which may affect business continuity is the type of the model that is used in eHealth services. In case this model is not client-centric, a client may easily have hundreds of separate, overlapping records in various systems and this limits the availability of information [4], a condition which affects client safety and leads to unnecessary duplication of tests and investigations, so it increases the cost of the services [3].

Lack of Interoperability

eHealth infrastructures include many diverse systems and applications interconnected at various scales e.g., a medical device collecting clinical data can be linked in the same network that a computer uses to access Internet [3]. A core issue for an effective and secure use of these services is to ensure a high level of interoperability and guarantee that information is transmitted safely through individual information systems, health service institutions, healthcare providers and clients [5] and, on the other hand, that the recipient's system is able to use the information received in order to proceed in various activities. For example, the terminology used in electronic health records must be based on universally applied standards and an agreed-upon framework or some open protocols for secure information exchange and services integration [3]. The lack of interoperability may also affect the security updates in an eHealth services network [3].

Access Control and Authentication

A major vulnerability in data security in eHealth infrastructures is sharing data between third parties and insiders, such as breaches by employees [6], indicating that access control and authentication is one key security features [3]. Users' identity authentication is necessary to ensure that they are authorized to access the system; an access control policy defines the information level that authenticated users are allowed to view or share [7]. Access control is a main safeguard for ensuring data privacy and integrity [8]. Within a centralized system with limited external connections, internal user access control becomes a higher challenge than external access control, whereas a distributed electronic health record or a mHealth chronic disease management system needs to prevent unauthorized access on data over the network [3].

The definition and enforcement of access rules for health data and services throughout clinical workflows is a precondition for any cooperative client treatment [3]. Despite strong authentication and access control, systems should be user-friendly avoiding errors introduced by the user [3]. A natural solution for providing strong access control to personal health records is to deploy attribute-based encryption (ABE). Therein data is encrypted cf. a key that depends on certain attributes or roles. Then anyone with a key that is associated with a matching attribute or role can decrypt the data. Attribute-based encryption is employed in a number of eHealth system architectures [9] [10] [11] [12] [13]. However, current solutions are still not efficient enough for real-world deployment and miss practical realizations of crucial features such as the protection of the access attributes and access pattern which both can be sensitive information itself and perform revocation of access rights.

Data Integrity

A common eHealth cyber security challenge is ensuring quality and integrity of the data that are stored and exchanged for clinical and administrative purposes: examples include clinical laboratory test results, client demographics, medication related information, radiology reports and images, pathology reports, hospital admission, discharge and transfer dates [3]. Errors in personal or clinical data may affect a person's medical treatment,

insurance or employability. Data integrity errors of eHealth are often related to incorrect entry by staff, incorrect conversion from a paper-based filing system to electronic health records and improper or insufficient use of standard based healthcare information exchange protocols [3].

Network Security

A fundamental challenge in securing eHealth infrastructures is considered to be network security, and according to ENISA study [3], this is highly related to many security incidents. Network security is critical when the security of other critical assets relies on the security of the network; being a top priority when the eHealth system is network based e.g., EHR/PHR and cross border eHealth [3].

A computer networks is a shared resource used by applications with different interests [14]. The Internet is a widely shared resource where a network conversation may be compromised by an adversary. In computer networks, an example of a passive threat, such as attempts to by an attacker to obtain information relating to prevailing communication, is that an adversary would eavesdrop on network communication. Active threats involve modifications of the transmitted data or the creation of the false transmission. Another active threat is that the traffic is unknowingly being directed to a false node such as a false host, a false router or a false website. Also, service providers can be attacked, e.g., websites may be defaced by remotely modifying without authorization the files that make up the website [14]. The rules that define who is allowed to do what are an issue of access control: cf., 'Access control and authentication'. The services may also be subjects to Denial of Service (DoS) attacks that unable to access to the service because of the overwhelmed bogus requests, being availability: cf., 'Systems availability'. The customer and the service also face threats from each other; each could deny a transaction to occur or invent a non-existent transaction. Nonrepudiation means that a bogus denial of a transaction can be disproved, and nonforgeability means that claims of bogus transaction can be disproved.

According to ENISA study [3], the main vulnerabilities of an eHealth network are the inadequate firewalls by 27% and place the external attackers as one of the major threats by 65% [6], while 81% health-care executives claim that their organizations experienced attacks by at least one malware, botnet or other cyber-attack during the past two years and only half feel that they are adequately prepared to prevent attacks.

Security Expertise and Awareness

While technical upgrades are important, minimizing human error is even more crucial because mistakes by network administrators and users—failures to patch vulnerabilities in legacy systems, misconfigured settings, violations of standard procedures—open the door to the overwhelming majority of successful attacks [15]. The security practices by health personnel are considered a source of potential problems and appear to be a significant challenge, as in some countries, like Austria, the human factor is considered the most important cause of security incidents [3]. Although risk assessment methods and information security plans and policies are currently an essential part of many organizations, the managerial aspects of information security still remain challenging, especially in emerging technological contexts. In the health sector, all relevant stakeholders must understand the security architecture and apply all the respective procedures. Management executives must understand information security requirements and importance. The security architecture and procedures must be well designed; organizational structure and especially the role of a security officer must be adequate. According to ENISA study [3], 20% of healthcare providers don't have a leader solely responsible for information technology security [6]. For example in Estonia, a security officer placement is an organizational structure mandatory by law only for public sector, and therefore many concerns are raised for the private sector security practices, since the lack of this asset may lead to misuse of security standards and a gap between security policy and work practices [16]. Quite often, the incentives for information security investments remain a black box, despite the fact that the lack of budget for information security solutions is repeatedly reported as a top challenge. A major concern regarding the lack of security expertise is that 23% of organizations do not have a security operations center to identify and evaluate threats [6].

Data Loss

The digitization of the healthcare industry is happening fast; a significant amount of vital, personal and confidential data are stored in digital format; and healthcare databases serve to replace the paper documents,

meaning that the protection of the data from loss is most important. Sometimes, a critical situation: e.g., software and hardware faults, network faults, security attacks, and natural disasters, happens, so data recovery and the timeframe that it can be achieved is closely related to data loss. Common causes of data loss are unauthorized access to clinical client data by IT vendors and by healthcare organizations personnel and the back-up policy [3]. However, according to CyberFactors (http://cyberfactors.com) healthcare records are five times as likely to be lost due to device theft/loss, because a third of healthcare employees work outside of the office or clinic at least once a week. A European Hospital Survey on benchmarking the deployment of eHealth services showed that 73% of the hospitals have an archiving strategy for long-term storage and disaster recovery, while 23% don't and only 14% are able to proceed to an immediate recovery and 42% in less than 24 hours [3].

Standardization, Compliance and Trust

According to ENISA study [3], one of the main concerns in attaining security in eHealth infrastructures is the proper use and persistence to create, maintain and enforce an interoperability framework so that integrated systems contributes to cost reduction in eHealth. The current distrust of the security of eHealth solutions is the main barrier towards their expansion, and cyber security is a prerequisite for a trust-building. Cyber security standards should be understood as a key enabler for the development and maintenance of co-created trust in the digital eHealth world [17].

Cross-border Incidents

Free movement of people is one of the cornerstones of the European Union (EU). According to the Directive on Cross-Border Healthcare which has been actual in the whole EU since 2013 for European citizens, no matter where they live, have the right to choose where to receive medical treatment across the EU, and to be compensated for it. However, in order to secure above-mentioned rights and unleash the potential of cross-border healthcare exchange, new solutions are needed to secure the storage and cross-border exchange of health data. The challenges that shall be tackled in order to facilitate transferability of data in cross-border healthcare are mainly related to building a common interoperability and access control and authentication framework [3].

Incidents Management

Incidents management is a major challenge in eHealth security because incidents that can be neither anticipated nor avoided exist. According to ENISA study [3], security incidents root causes include human errors (31%), system failures including third party failure, e.g., hardware failure (31%), malicious actions such as DDoS attack, MITM attacks, etc. (15%), natural phenomena (8%), and miscellaneous (15%). The study expresses the need for (1) eHealth organizations to have an incident response capacity, in order to timely identify incidents and restore and reconstitute systems and services in a trusted manner, and (2) a pan European-level incident reporting, classification and alerting mechanism [3].

TOWARDS THE PARADIGM OF EHEALTH CYBER SECURITY

Design Aspects of eHealth Critical Information Infrastructure

The research data of this study (described in appendix) is in line with EC Directive on Critical Infrastructures (2008/114/EC); revealed outcome is that healthcare services are in a critical societal sector and therefore eHealth systems have to be considered as critical information infrastructures (CII) that should be protected from all types of threats, including cyber security attacks. This outcome is also in line with the Network and Information Security (NIS) Directive in which healthcare is considered one of the critical sectors vital for the society; and most eHealth security challenges are equal to all critical information infrastructure protection (CIIP) issues [3] whose main complication is the lack of resilience, typically losing essential functionality following adverse events [18]. Figure 2 comprises the variety of key design aspects in sociotechnical Cyber-Physical Systems.

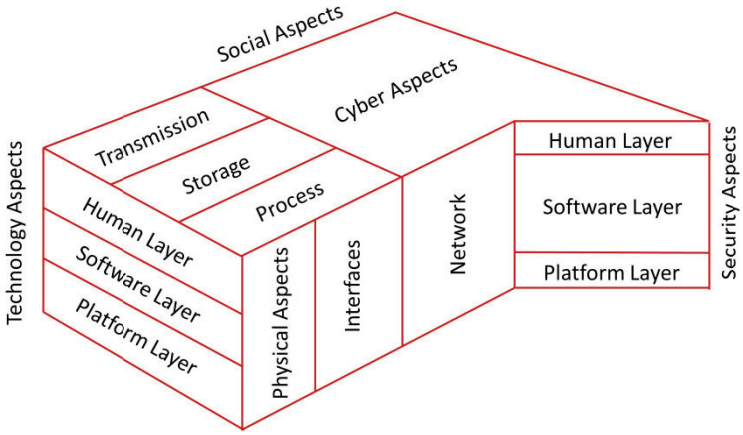

FIGURE 2. Variety of key aspects in sociotechnical Cyber-Physical Systems

Modern societies' critical infrastructures are sociotechnical cyber-physical systems (CPS) [19]. Past sociotechnical systems were physical systems, including the human layer and the platform layer; and current sociotechnical systems are software-intensive systems (SIS) as shown in Figure 2. SIS' future trend is that the software layer (=cyber part) is growing [20] as illustrated in the view from left to right hand side in Figure 2. All SIS are also cyber-physical systems: human and platform layers form the physical part and the software layer forms the cyber part of the CPS. Figure 2 demonstrated that cyber aspects can be seen as relations with social aspects. Instances of CPS are being developed that are part of a globally networked future world, in which eHealth related products, equipment and objects interact with embedded hardware and software beyond the limits of single applications, e.g., with the help of sensors, Internet of Things, Data and Services.

Design Aspects as a Sense of Resilience

The study revealed that our society's critical CPS, such as communication, energy, water, transportation and healthcare include lacks of resilience, typically losing essential functionality following adverse events [18]. It is noteworthy that Linkov et al. [18] describes the term "resilience" as a property of a system, deserving transition from just a buzzword to an operational paradigm for system management.

In the eHealth context, identifying the need for system resilience requires defining the system; here, revolutionary advances in hardware, networking, information and human interface technologies which require new ways of thinking about how CPS are conceptualized, built, improved and evaluated. Then, the outcome of study as a sense of resilience is compiled in Figure 3.

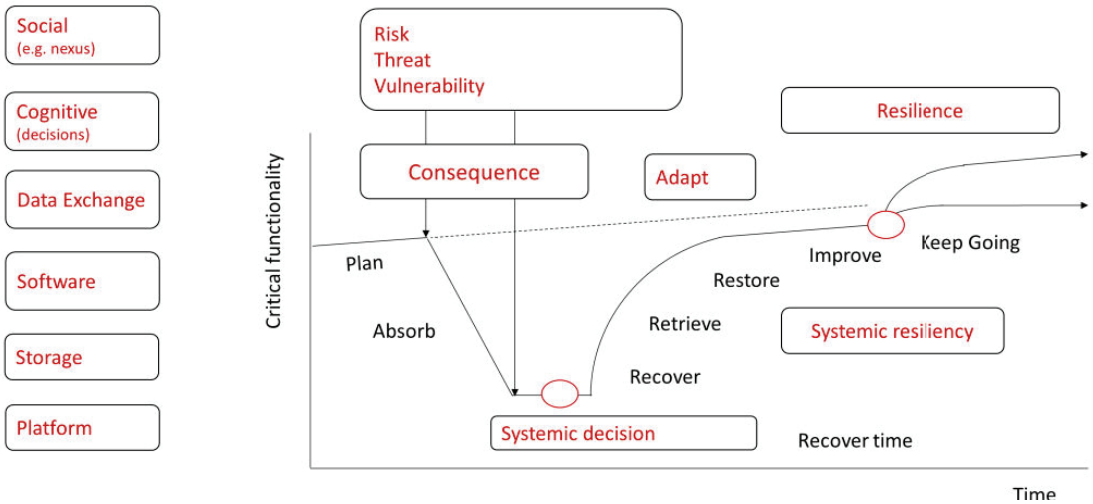

FIGURE 3. Compiled aspects of a Sense of Resilience

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

Then, a sense of resilience addresses to the ability of a system, community or society exposed to security-safety related threats to resist, absorb, accommodate to and recover from the effects of a threat in a timely and efficient manner; including through the adaption, preservation and restoration of its essential basic structures and functions; and commitments to the decisions and adaptions to still keep going.

Design Aspects for Sociotechnical Cyber-physical Systems

The last inference of this study is focused on the cyber resilience governance framework and design aspects for eHealth, which are based on recent settings of sociotechnical, cyber-physical, software-intensive and systems of systems in references [22] [17] [23] [24].

The Network-Centric Warfare (NCW) doctrine [25] identifies four domains that create shared situational awareness and inform decentralized decision-making; cf. Figure 1 extension and Figure 3 above and Figure 4 including: 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.

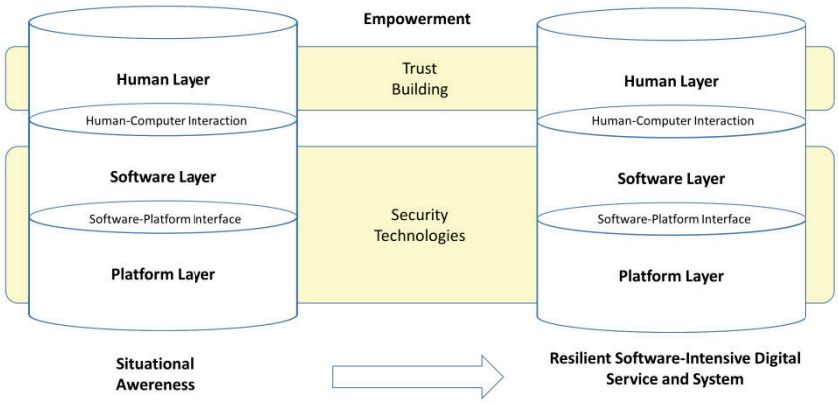

FIGURE 4. Design aspects for resilient eHealth systems

The continuum of a design theory for resilient CPS can be a useful method for communities to share knowledge and best practices utilizing a common frame of reference, design and resilience aspects, cf. [19] and [21] and Figure 4. Linkov et al. [26] combined the event management cycles and NCW domains to create resilience metrics for cyber systems. Their approach integrates multiple domains of resilience and system response to threats through integrated resilience metrics; however, study of systems as multi-domain networks is relatively uncommon. Links across domains are likely to affect the network's resiliency and should be assessed using network science tools [27].

According to this study, the term "resilience" in cyber domain would address to that a system is able to adapt to changing conditions based on run-time situational awareness, and a priori risk analysis when possible. Situational awareness (can be a software-intensive system itself) involves being aware of what is happening to understand how information, events, and one's own actions affect the goals and objectives, both now and in the near future. The most important enablers of situational awareness are observations, analysis, visualization, and cyber-policy of the government. Security technologies include all technical means towards cyber security, such as secure system architectures, protocols and implementation, as well as tools and platforms for secure system development and deployment.

Security management and governance covers the human, organizational and cognitive aspects of information security. Its focus areas include: Security policy development and implementation, and information security investment, incentives, and trade-offs. Information security management system (ISMS) focuses on continuously

managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity and availability of the organization's information assets that do preserve. Cognitive aspects run around the framework; all technical and human components should learn from prior events and incidents, see [22] [17] [23] [24].

Digital service driven progress brings opportunities across many sectors but also vulnerabilities to cyber-physical systems and related digital services. In the target scale of European-Global healthcare, there is a need for eHealth information nexus being one example of a safety-critical decision based networked system on cross-border secure and safe information exchange and common eHealth information sharing democracy and digital citizen's empowerment. In order to achieve the trust of users, measures of safety and security should be taken into consideration in line with the aspects of privacy by design and citizens' digital empowerment.

DISCUSSION

In the perspective of resilience, risk analysis and risk management based on probabilistic quantitative methods have been widely adopted and have been useful for dealing with foreseeable and calculable stress situations of any critical infrastructure. Benchmarks and thresholds for risk analysis are built into the regulations and policies of organizations and nations; however, this approach is no longer sufficient enough to address the evolving nature of risks in the eHealth world [18].

Therefore, resilience should be integrated into the design of eHealth systems, and new co-creative policy-regulatory structures of systems management to address the emerging issues associated with complexity and uncertainty should be furthered and studied. This urgent need exists to complement the existing knowledge base of risk analysis and management by further developing frameworks and models enabling system-wide and network-wide resilience analysis, engineering and management.

Channels of communication for transparent dialogue on resilience governance with stakeholders should be established for the timely and broad acceptance of resilience concepts. By applying privacy by design framework and developing privacy-friendly and strong access control methods, then it makes it more possible to store personal health records in the most secure and privacy-friendly way.

CONCLUSIONS

In this study, the high level of interconnectivity was found in the cases of eHealth related cyber-physical systems which has opened many paths and path-dependencies for cyber-attacks, including internal and external threats and vulnerabilities within supply chain and cross national border transaction networks. Despite continual progress in managing risks, it is clear that current prevention of all possible attacks and malfunctions is not enough for current or future cyber and infrastructure systems.

As final remarks of this study: eHealth information exchange can be proficient with the capacity to make a significant and positive difference in healthcare delivery. This depends upon an appropriate legal regime, mutual policy creation, valid information and privacy measures, and the deployment of strategies to deal with human factors and empowerment to find the correct balance in relationships between the relevant institutions and individuals.

APPENDIX

The data collection of this study was cumulative, from real-world projects that the authors participated in during the course of 15 years, and data collection was systematically used for analysis. The data collection included the following themes: data of real implementations (n=9); management data (n=52) files, which includes specifications, strategies, and legislation; data of development days (n=50) files, which includes data displays, notes, development proposals, and reports (including test reports); and feedback data from users' (n=15) description files; and detailed literature in review (n=40) references.

REFERENCES

1. National Training Standard for Information Systems Security (INFOSEC) Professionals, NSTISSI, 1994.
2. T. Sahama, L. Simpson and B. Lane, "Security and Privacy in eHealth: Is it possible?," *IEEE 15th International Conference on e-Health Networking, Applications & Services (Healthcom),* pp. 249-253, 2013.

3. D. Liveri, A. Sarri and C. Skouloudi, "Security and Resilience in eHealth: Security Challenges and Risks," European Union Agency For Network And Information Security, Heraklion, Greece, 2015.
4. L. Røstad and Ø. Nytrø, "Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges," in *The Second International Conference on Availability, Reliability and Security*, 2007.
5. E. AbuKhousa, N. Mohamed and J. Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges,," *Future internet,,* 2012.
6. "Health care and cyber security: Increasing Threats Require Increased Capabilities," KMPG, 2015.
7. R. Gajanayake, R. Iannella and T. Sahama, "Privacy Oriented Access Control for Electronic Health Records," in *Data Usage Management on the Web Workshop at the Worldwide Web Conference, ACM*, Lyon, 2012.
8. L. Røstad, Access Control in Healthcare Information Systems, PhD Thesis, Trondheim: Norwegian University of Science and Technology, 2009.
9. L. Ibraimi, M. Asim and M. Petko, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," in *6th InternationalWorkshop onWearable Micro and Nano Technologies for Personalized Health (pHealth)* , 2009.
10. M. Li, S. Yu, K. Ren and W. Lou, "Securing Personal Health Records in Cloud Computing: Client-Centric and Fine-Grained Data Access Control in Multi-owner Settings," in *SecureComm 2010*, Heidelberg, Springer, 2010, pp. 89-106.
11. M. Li, S. Yu and Y. Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems,* vol. 24, no. 1, pp. 131-143, 2013.
12. S. Narayan, M. Gagne and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *ACM workshop on Cloud computing security workshop*, New York, 2010.
13. A. Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Secure Medical Architecture on the Cloud Using Wireless Sensor Networks for Emergency Management," in *Eighth International Conference on Broadband and Wireless Computing, Communication and Applications*, 2013.
14. L. Peterson and B. Davie, Computer Networks: A Systems Approach, 5th edition, Burlington: Elsevier, 2012.
15. J. Winnefeld, C. Kirchhoff and D. Upton, "Cybersecurity's Human Factor: Lessons from the Pentagon," *Harvard Business Review,* 2015.
16. P. Williams, "When trust defies common security sense," *Health Informatics Journal,* 2008.
17. J. Rajamäki and J. Knuuttila, "Cyber Security and Trust: Tools for Multi-agency Cooperation between Public Authorities," in *in Proc. of The 7th International Conference on Knowledge Management and Information Sharing - KMIS*, Lisbon, 2015.
18. I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs and T. Thiel-Clemen, "Changing the resilience paradigm," *Nature Climat Change,* vol. 4, pp. 407-409, 2014.
19. J. Rajamäki, "Towards design theory for resilient (sociotechnical, cyber-physical, software-iontensive and systems of) systems," in *10th International Conference on Computer Engineering and Applications (CEA '16)*, Barcelona, 2016.
20. A. Hevner and S. Chatterjee, Design Science Research in Information Systems, Springer, 2010.
21. Disaster resilience: a national imperative, National Academy of Sciences, 2012.
22. J. Rajamäki, "Towards a design theory for resilient (sociotehnical, cyber-physical, software ans systems of) sytems," in *10th International Conference on Computer Engineering and Applications (CEA '16)*, Barcelona, 2016.
23. J. Rajamäki and R. Pirinen, "Critical infrastructure protection: Towards a design theory for resilient software-intensive syst,," *European Intelligence and Security Informatics Conference (EISIC),* 2015.
24. R. Pirinen and J. Rajamäki, "Mechanism of Critical and Resilient Digital Services for Design Theory," in *The 2nd International Conference on Computer Science, Computer Engineering & Social Media, IEEE*, Lodz, Poland, 2015.
25. D. Alberts, Information age transformation, getting to a 21st century military. DOD Command and Control Research Program, 2002.
26. I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen and A. Kott, "Resilience metrics for cyber systems," *Environ Syst Decis,* 2013.
27. T. Abdelzaher and A. Kott, Resiliency and Robustness of Complex Systems and Networks. Adaptive, Dynamic and Resilient Systems, Florida: Auerbach Publications, 2013.