Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 72 (2023) 2604–2611

Transportation Research Procedia

www.elsevier.com/locate/procedia

Transport Research Arena (TRA) Conference

Including the excluded: how can design of digital delivery service address cybersecurity concerns of vulnerable users

Andrea Capaccioli[a]*, Luca Urciuoli[b], Floridea Di Ciommo[c], Gianni Rondinella[c], Sabina Giorgi[a], Rebecca Hueting[a]

[a]*Deep Blue srl, Rome, Italy*
[b]*MIT-International Logistics Programme, Zaragoza Logistics Center, Zaragoza, Spain*
[c]*cambiaMO|changing Mobility, Madrid, Spain*

Abstract

The paper discusses co-design as a fundamental approach to increase security and inclusivity of digital mobility and delivery services. Main threats for vulnerable users of a selected digital delivery platform in Madrid are expounded, together with necessary cybersecurity practices to be considered at design-stage. The paper presents the results from a pilot in Madrid, part of the INDIMO H2020 project. The focus is on the creation of cybersecurity and privacy guidelines, and their use for the re-design of digital mobility services. A series of recommendations are identified to be implemented in the short and long-term, covering both organizational and technological challenges, among which implementing processes for responding to data breaches and inform users, and having transparent privacy policy. Vulnerable users will benefit from an augmented level of service inclusiveness.

Keywords: cybersecurity; digital mobility services; inclusivity; co-design; personal data protection; privacy;

1. Introduction

The scope of this paper is to discuss the concept of co-designing as a fundamental approach to increase security and inclusivity of digital mobility services. Main threats for vulnerable users of a selected digital delivery platform in Madrid (Spain) are presented, together with recommendations about how cybersecurity practices will need to be shaped accordingly at design stage. The paper is based on the work done as part of the INDIMO H2020 project (Giorgi et al., 2021). The project applies a user-centric approach to improve inclusiveness and equity of digital mobility and

* Corresponding author. Tel.: +39-3477307309
E-mail address: andrea.capaccioli@dblue.it

10.1016/j.trpro.2023.11.791

delivery services, through the design of a specific toolbox which includes: Universal Design Manual for digital mobility services, Universal Interface Language for the use of icons and design of interfaces, Guidelines for Cybersecurity and Personal Data Protection (CSG), Policy Evaluation Tool. The toolbox has been applied and evaluated, in 5 different project's pilot sites (i.e., Emilia Romagna, Flanders-Antwerp, Galilee, Madrid, Berlin).

This paper focuses on the implementation of the Guidelines for Cybersecurity and Personal Data Protection (CSG), discussing the results from the Madrid pilot site. By analysing the pilot's experience and the development of CSG the following research questions were addressed:

- How to consider citizens' inclusion when shaping cyber-security practices for digital mobility services?
- How can a co-design approach help to increase security and inclusivity of digital mobility services?

First, the main challenges for inclusiveness related to cybersecurity are introduced, making visible the role and the importance of considering human factors for a more inclusive and efficient cybersecurity approach. Then, the general co-design methodology developed in the INDIMO project is described, together with the risks assessment process followed for the CSG development. As next step, the Madrid pilot's experience is discussed, highlighting the results of the co-design and risks assessment process, and the impact on the cybersecurity and data protection. From there, conclusions are draw.

2. Cybersecurity challenges for inclusiveness

Cybersecurity comprehends the practices to secure electronic equipment like computers, servers, mobile devices, networks etc. from antagonist threats (Urciuoli et al., 2013; Kaspersky, 2020). Within the area of digital solution for transport mobility, personal data of public transport users could be stolen from the servers of central agencies that share and collect information from smartphone applications. Personal data information and payment subscription fee, information about location and transactions can be illegally taken from RFID based electronic tickets (Radio Frequency Identification tags) that currently are used by many European cities. The same cards could be skimmed or manipulated to create illegal subscriptions (Sadeghi, Visconti, & Wachsmann, 2008).

These challenges become more critical when considering vulnerable people as end-users. It has been shown that lack of technical skills, physical impairments or language limitations make vulnerable users more at risk of cyberattacks (Sonowal et. al., 2017). A breach and an attack could expose them to repercussion higher than for other users (e.g., like in some extreme cases where this could be an issue of physical security or discrimination for minorities). Hence, a carefully designed and implemented data protection and cybersecurity strategy become even more important when there is the involvement of vulnerable categories of users. The need for a holistic security-based approach in smart cities, considering human, societal and technical dimensions in cybersecurity, has been discussed in previous research (Habibzadeh et al., 2019; Nai et al., 2020).

These considerations are expected to convey into the development and implementation of inclusive services that address the cybersecurity challenges of vulnerable users. Parsons et al. (2017) defined the human factor as "*the first line of defence*" against threats, hence the response and preparedness to attacks is improved by considering the role of people in the cybersecurity scenario. Pollini et al. (2021) defined a clear framework that take into consideration human factors as the strategic link for security in an organization, considering three main factors: the individual, the organizational and the technological in a "holistic" approach. Non-technical countermeasures can be taken, together with the technological protective measures usually recommended. Among the first ones Pollini et al. (2021) identified:

- Adopting user-centred design approach to promote and implement usable rules and practices;
- Improve the usability of tools supporting work specific needs ensuring that their compliance with security restrictions does not jeopardize the user experience;
- defining security policies and training campaigns that use a customised approach commensurate to the knowledge and skills of the employees and targeted to specific information security areas (example dividing among IT people and non-IT people).

Security mechanisms should not make it difficult to perform the main task, but technologies, and so also implementation of security features, must be designed to fit users' physical and mental abilities (Sasse, 2015). Considering the involvement of vulnerable categories of users that could be exposed to attack and breach with repercussion higher than for other users (e.g., in case of possible discrimination or even physical security), it is

essential for designing an effective data protection and cybersecurity strategy. From this perspective, the privacy by design principles (Cavoukian, 2011) and the privacy design strategies (Hoepman, 2014) are approaches to data security and privacy that follow this approach. The privacy by design principles suggested by Cavoukian (2011) address the impact of ICTs technologies by focusing on making privacy the default mode of operation for organizations. They are general principles for organizations, designers and developers that aim to prioritise privacy. In a more operational way, Hoepman (2014) defined the privacy design strategies also considering the emerging data protection legislation at the time. The scholar provided a practical approach towards the implementation of data privacy, also focusing on technologies that can enhance privacy. These two approaches, together with the previously presented issues and reflections, inspired the work of drafting the CSG, which will be discussed in the next sections of this paper.

3. Methodology

In this section, the overall co-design methodology used in the INDIMO project is presented first, followed by the methodology for the cybersecurity and privacy risks assessment applied to collect data from the project pilots, and to define the CSG.

3.1. The INDIMO co-design methodology

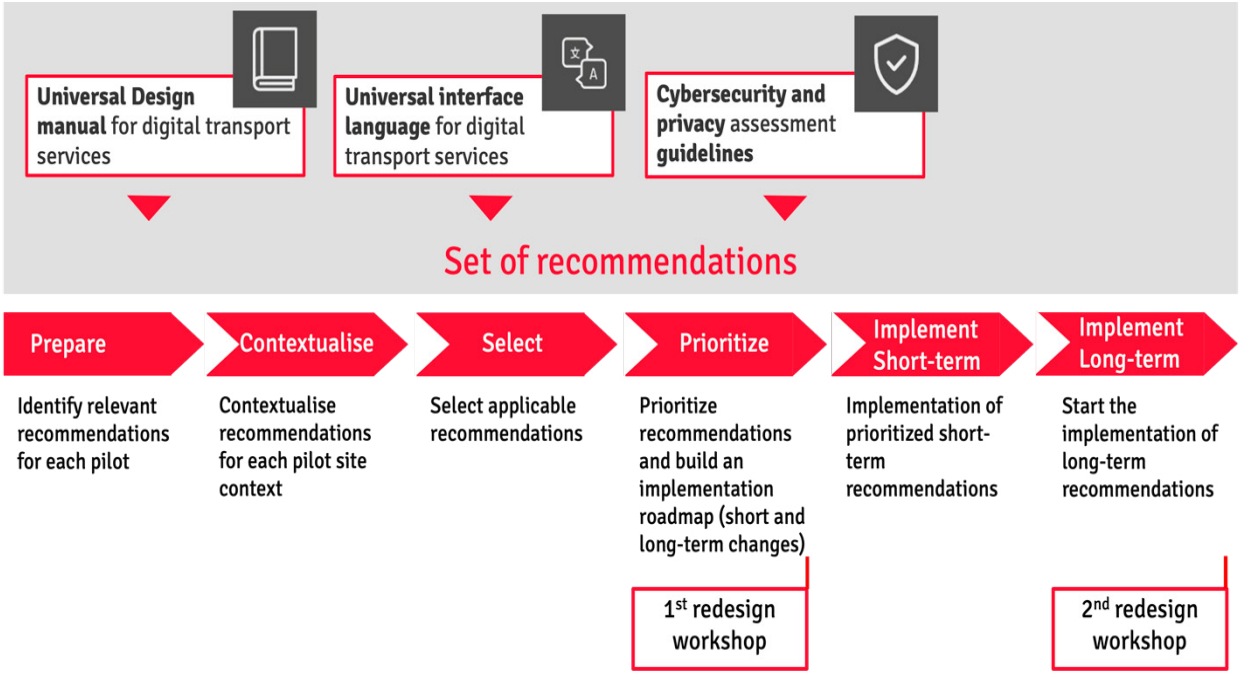

Fig. 1. Project co-design process stages and activities

The development and implementation of CSG are part of a 5 stages co-creation process developed in the INDIMO project. The main stages of the process are: 1) UX Research, i.e., identification of user and non-user needs, and also needs and concerns of developers, policy makers and mobility operators; 2) Co-design of the project toolbox (Universal Design Manual, Universal Interface Language, Guidelines for Cybersecurity and Personal Data Protection, Policy Evaluation Tool), among which the CSG; 3) Co-implementation of CSG, together with the other tools of the INDIMO toolbox in the five pilots of the project. It consisted in re-designing pilots' digital mobility and delivery solutions based on the toolkit implementation; 4) Co-evaluation, i.e., feedback and refinement of some of the tools developed. This stage is not applicable to the CSG, since they do not have a second improved version; 5) Project

results strengthening, i.e., transformation of the INDIMO toolkit in an online version accessible to all. This process has been used as a general framework to design and implement the project toolkit, also including the CSG.

The co-implementation phase consisted of co-design activities, where users and non-users, developers, service operators, users' representatives and policy makers were engaged in identifying the main changes to be implemented by applying the recommendations based on the project's toolkit (see Fig.1). The changes, based on the recommendations, were divided into short-term and long-term changes, which were implemented during two iterative co-design cycles of INDIMO project's activities. The identified relevant short-term changes were discussed in a dedicated first re-design workshop to agree on solutions and implementation plan. After the first iteration, a second re-design workshop focused on long-term recommendations to be implemented in the second phase of project activities, which will be evaluated after their complete implementation during summer 2022.

3.2. The risks assessment methodology

The cybersecurity guidelines were generated from the results of a risk assessment questionnaire conducted in the five project pilot sites. Among them, the Madrid case study can be considered as particularly significant for the many characteristics defining it: the organization delivering the service is a small cooperative; the organization developing the application is part of a network of cooperatives developing services focusing on sustainability, workers' rights, and social impact; it covers a variety of vulnerable users engaged in the pilot activities by the project partner responsible for it. The questionnaire was developed in two steps:

1) A review of cybersecurity standards proposed by ISO27001 and the National Institute of Standards and Technology, NIST 800-55. The selection of these standards was motivated by existing literature explaining that ISO27001 is one of the most known and diffuse standard available. Yet, these guidelines are more technical and are expected to fit mature organizations with well-established processes or products (Auditboard, 2021). Pilots were at different level of maturity, both in terms of technologies, services and in terms of operations and organizational maturity. Hence, following internal meetings with INDIMO risk management team, it was decided to adopt part of ISO27001standard and integrate it with the NIST framework (Chew et al., 2008). Additional materials to prepare the questionnaire was requested from the case study, covering any of the following topics:

- IT architecture of the system;
- Data management plans;
- Risk management plans;
- Enforced regulatory frameworks;
- Overall cybersecurity strategies and policies applied;
- Other relevant documentation that could be used to contextually describe the cybersecurity state-of-play in the organizations involved in the pilots.

2) The second step consisted of testing the questionnaire with 2 selected experts in cybersecurity. Thereafter, the questionnaire was further revised, improved, and thereby used to collect data from the different pilots, among which the Madrid pilot. The final version of the questionnaire is available in Appendix A of this paper, and it includes the following sections:

- Managerial processes to plan and improve cybersecurity;
- 3rd parties involved and main data exchange;
- Risk assessment measured as impact and likelihood;
- Threats involving users with special needs;
- Protective measures;
- Efficiency/effectiveness KPIs.

The answers were requested via e-mail, and video conference meetings were organized to discuss any doubts raised after an initial review of the material.

4. Cybersecurity guidelines and their implementation, the Madrid pilot

The main results achieved consist of a set of guidelines for improving cybersecurity and personal data protection in digital mobility services. The guidelines are meant to be used for design and re-design of services with a security

by design approach, and for increasing awareness among users about digital data protection and security. The guidelines focus on the following pillars:

- Establish processes and procedures: even if an organization is not certified ISO27001, implementing plan-do-check-act style process is a key factor to consider for security;
- Consider human factors and phishing prevention: human factors are the "first line of defence" (Parsons et. al., 2017). Understanding the reasons of errors or violations is important to create a security culture within an organization;
- Evaluate risks connected to third parties' services: services can heavily rely on third party services, assessing the security of such components, and understand how to mitigate possible attacks to third parties is important to improve security and avoid major disruption of services;
- Design services thinking ahead of their maintenance: when designing the system, it must be considered its maintenance, and the possibility for quick update and fix of identified vulnerabilities. A continuous check, and update is more effective than larger security patches;
- Systemic monitoring: data traffic monitoring and intrusion detection systems are important to prevent and react faster to attacks and intrusions to the systems;
- Enable smart data collection from users: data from users should be collected only if necessary for the service. Designing how to collect few personal data and, at the same time, being able to provide the same service to all groups of users would help the security and reducing risks. At the same time, is important to develop transparent documentation and policies for users to address data security and ethical concerns. This can be done using summaries and checklists;
- Physical security: if physical IoT (Internet of Things) devices are deployed for managing the service, it is important to implement anti-tampering solutions to prevent physical sabotages and attacks coming from direct access to devices;
- Design for inclusivity: implementing inclusive design features help distinguish malicious sources from authentic ones, increasing the security also of vulnerable groups such as the one considered in the Madrid pilot, and make them able to act and recognize threats. The toolkit designed within the INDIMO project, also including the CSG, is a tentative to provide practical ways of increasing inclusivity and thus also cybersecurity.

4.1. The Madrid pilot case risk assessment

The Madrid case is about the Cycle logistics platform for delivery healthy food, provided by La Pájara, a small delivery goods and food cooperative established in 2017. The service is based on a digital platform operated by CoopCycle, a non-profit federation of 64 small delivery goods and food cooperatives, including 62 in Europe and in Canada, all of them sharing a common digital platform to physically operate the service at their locations. The main aim of the Madrid pilot is to improve accessibility of vulnerable groups of people to healthy food using a digital delivery platform. Several vulnerable groups are considered (i.e., older people, lower income people, people with reduced mobility, people lacking digital skills, people with mental health impairments, people with visual impairments) that may experience issues in using digital platforms and then, also they could experience, as discussed, increased security threats.

Main threats for vulnerable users have been identified through the application of the methodology described in section 3. From the risk assessment performed through the questionnaire (see section 3.2), also including an interview with one of the main developers of CoopCycle, emerged that the small dimension, and the cooperative form, which made the organization more horizontal and informal prevent the establishment of formal managerial processes to govern cybersecurity. The company follows standards and best practices ensuring that relevant software applications are regularly updated. At the same time, CoopCycle demonstrated how the vision of future maintenance is included in the services' design-stage.

The overall CoopCycle approach puts a lot of attention to ethical issues, with a particular focus on users' privacy: they choose to not share users' data for marketing analysis and there are no cookies for data analytics on the CoopCycle app. The only minimum sharing of users' information is through the Facebook social login which is present in the browser version of the service. At the same time, particular attention is paid to third parties' usage, where the main

critical third parties services are Stripe for payments management and geocoding APIs for geolocation. These two services could pose risks for possible data breaches, but they offer an essential service for the app. The unauthorized access to information shared with suppliers is a risk that has been identified with medium probability and medium impact. The lack of redundant systems in case of data breach or major disruption was considered as one of the highest risks identified during the assessment.

4.2. Recommendations selection and re-design

During the 1st iteration of co-design activities, participants to the re-design workshop defined the main roadmap of short and long-term recommendations to be implemented in the pilot during the project. Together with the general guidelines from the INDIMO toolbox, the risk assessment highlighted some specific recommendations for the Madrid pilot about cybersecurity and data privacy. These are relevant also taking into consideration the possible service growth and a scale up of the CoopCycle app to serve more cooperatives, cities, and users. The main recommendations are the following:

- The implementation of standards and guidelines developed in ISO28000 or NIST800 are recommended;
- Usage of technologies for detecting intrusion anomalies, e.g., online scanners, and pen-testing software;
- Integrate payments with external providers, to take advantage of their security solutions;
- Establish processes/routines to control possible mistakes of CoopCycle employees and/or respond to incidents. Perform auditing and drills;
- Establish rules for usage of external devices (e.g., usb devices, personal devices, etc…) at work/home;
- Use backup systems to ensure redundancy;
- Create a process for a prompt and shared reaction in case of data breach and inform users to increase trust;
- To address possible ethical issues connected with the data security aspects, it may be worth to work on specific strategies such having transparent privacy policy.

During the re-design workshop activities, a participant who is both a user of the service and a developer with reduced vision, proposed to work on the language used in the legal policies presented on the website, especially the privacy policy. It has been proposed to check the language and make it more accessible for users by means of a simplified version understandable by everyone. Thus, all users could be informed not just in a formal way, by making available the policies that are usually not read. The person proposing this, also offered to check the legal text and to reformulate it. CoopCycle agreed-upon the suggestion, and a team of two persons, one representative of the users and one from La Pájara was established to work on this recommendation. The team started also to work on the translation into Spanish of all the legal notices that were available only in English and French. This activity resulted in the reformulation of the privacy policy and other legal notices into a transparent language, understandable and easy to access for all users, especially from vulnerable ones.

For what concern the long-term implementation, participants involved in pilot activities did not select any other recommendations regarding cybersecurity and data privacy. The current focus is on activities regarding the recommendations coming from the other tools of the project, i.e., Universal Design Manual and Universal Interface Language. The future implementation of both organizational and technological recommendations is relevant to create a cybersecurity culture in the organization, but also shared with users to address the main threats that, especially the most vulnerable ones, they could experience accessing the service. Developers of CoopCycle acknowledged the relevance of the more technical recommendations regarding cybersecurity, and they are considering them for the future development of the app, even after the end of the project.

5. Discussions and conclusions

Among the different pilots involved in the INDIMO project, the Madrid case study allowed to highlight how inclusion and accessibility are relevant for cybersecurity. Pilot's participants (i.e., users, users' representatives, policy makers, developers) evaluated and prioritized several recommendations during the co-design workshops and created the timeline for implementing short and long-term changes to the service. Among the considered recommendations,

one related to cybersecurity has been recognized important for improving the CoopCycle app toward a more inclusive digital delivery service that wants to make vulnerable users more aware of data privacy and security. Users themselves discussed the relevance of cybersecurity and data privacy and made explicit the need for implementing transparent policies. Delivering transparent policies, with easy-to-understand language is a way to help inclusion, to increase the knowledge and awareness of the use of personal data, and the rights of people to have their data secured.

The general objective of the co-design activities in the Madrid pilot was to include vulnerable groups into the use of a digital delivery service which could support them in providing healthy food, reducing barriers at the access due to lack of developments requirements in a previously developed version of the application. Lowering barriers, means also increasing trust, and creating a digital environment where the user experience is improved and thus users can feel safe. This is especially difficult if considering people who lack familiarity with digital tools, older people, or people with impairments. Hence, the establishment of the co-design process based on the creation of a stable community of users, users' representatives, and others interested stakeholders, is of major importance for creating and implementing the cybersecurity recommendations identified during the project. Engaging users is a way to create a more inclusive and more secure services.

As a next steps and future activities for the Madrid pilot, it is important to sustain the continuity of the co-design process to implement the identified recommendations (see section 4.2), and to shape with the users the right intervention for creating trust and security, while having an inclusive and accessible experience. The creation of a shared cybersecurity culture within the organization is an important result that could be achieved by implementing a long term organizational strategy integrating our recommendations. Especially considering the establishment of processes and procedures for controlling possible mistakes and respond to incidents, which need specific training for employees. At the same time this needs to go together with the establishment of a risk management approach to address possible data breaches, also from the side of communicating to users, thus increasing the trust. Those organizational aspects should be aligned with technological upgrades / implementations, e.g. systems for intrusion detection, and data , e.g., backup systems.

Guidelines created by the INDIMO project, which are presented in this paper, are a tool that can be also applied to other cases where digital mobility solutions are being developed, and where users can be a strong driver of innovation.

Acknowledgements

Research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 875533 (INDIMO project).

Appendix A. Risk assessment questionnaire

1. Do you have any managerial improvement cycle applied for cybersecurity / risk management? If so, can you illustrate the activities in the following phases, PLAN-DO-CHECK-ACT (see figure below)? If a formal process cycle does not exist, what is the rationale? What tacitly defined informal steps are usually taken to respond to cyber security challenges?
2. Describe the 3rd parties' actors enabling the pilot's services, and (if possible) what sensitive data is exchanged?
3. Rate the following risks probability (from 1 very low to 5 very high) and impact (from 1 very low to 5 very high) for your pilot:

Risks related to human failures / mistakes of resources employed, (e.g., In-house staff deviating from the process, staff at supplier side making mistakes/falling for social engineering attack, Failure of processes such background screening

Corruption / malware mobile devices at work/home

Malware / virus in media devices, e.g. physical media transfer devices used by employees

Unauthorized access to network and network services.

Risk for physical access, damage and interference to the organization's information and information processing facilities.

Sabotage of equipment/devices used for the storing / exchange of information.

Backup system failure.
Lack of redundant systems causing a major disruption or data breach
Unauthorised use of credentials allowing access to information systems.
Risk for eavesdropping, intrusion via wireless networks and information theft.
Lack of security requirements in purchasing/procuring of new information systems or updates of existing ones.
Unauthorized access to information shared with suppliers.
Lack of response practices in case of cyber security / breach into the system.
Unauthorized physical access to premises (to steal or destroy devices or data)

4. Are there any additional cyberthreats (including data loss/privacy issues) that you would like to add? Are there any specific threats targeting users with specific needs and limited access to the services implemented in your pilot? In case describe them and rate their probability and impact as the one above.

5. What protective measures are being adopted by your organization to prevent and counteract cyberthreats / unauthorized access to your systems / data loss?

a. Are there any additional security measures that should be implemented to protect more vulnerable segment of users, i.e., specific needs and limited access.

6. Can you elaborate how the following KPIs can be affected in case of a successful cybersecurity attack against your pilot? A. Costs; B. Brand Image; C. Sales/Profits

References

Auditboard, (2021), NIST vs. ISO: What's the Difference? https://www.auditboard.com/blog/nist-vs-iso-whats-the-difference/ (last consulted January 2022)

Cavoukian, A. (2011). Privacy by design. The 7 Foundational Principles. Technical report, Information and Privacy Commissioner of Ontario

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). Performance Measurement Guide for Information Security. US department of Commerce.

Giorgi, S., Hueting, R., Capaccioli, A., di Ciommo, F., Rondinella, G., Kilstein, A., Keseru, I., Basu, S., Delaere, H., Vanobberghen, W., Bánfi, M., & Shiftan, Y. (2021). Improving Accessibility and Inclusiveness of Digital Mobility Solutions: A European Approach. In N. L. Black, W. P. Neumann, & I. Noy (A c. Di), Proceedings of the 21st Congress of the International Ergonomics Association (IEA 2021) (Vol. 220, pagg. 263–270). Springer International Publishing. https://doi.org/10.1007/978-3-030-74605-6_33

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660. https://doi.org/10.1016/j.scs.2019.101660

Hoepman, J.-H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (A c. Di), ICT Systems Security and Privacy Protection (Vol. 428, pagg. 446–459). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_38

Kaspersky. (2020). What is cybersecurity. Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lucas, K., Martens, K., Di Ciommo, F., & Dupont-Kieffer, A. (Eds.). (2019). Measuring transport equity. Elsevier.

Nai Fovino I., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., Tirendi S., Cybersecurity, our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1, doi:10.2760/352218, JRC121051.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Pflügler, C., Schreieck, M., Hernandez, G., Wiesche, M., & Krcmar, H. (2016). A concept for the architecture of an open platform for modular mobility services in the smart city. Transportation Research Procedia, 19, 199-206.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work. https://doi.org/10.1007/s10111-021-00683-y

Sadeghi, A.-R., Visconti, I., & Wachsmann, C. (2008). User privacy in transport systems based on RFID e-tickets. PiLBA'08 Privacy in Location-Based Applications, 102-121.

Sasse, A. (2015). Scaring and Bullying People into Security Won't Work. IEEE Security & Privacy, 13(3), 80–83. https://doi.org/10.1109/MSP.2015.65

Sonowal, G., Kuppusamy, K. S., & Kumar, A. (2017). Usability evaluation of active anti-phishing browser extensions for persons with visual impairments. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 1–6. https://doi.org/10.1109/ICACCS.2017.8014654

Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security–potential threats. Information & Security: An International Journal, 29(1).