pHealth 2024
M. Giacomini et al. (Eds.)

doi:10.3233/SHTI240087

Stakeholder Perception's of Cybersecurity for Welfare Technology and Remote Care Devices

Alvhild Skjelvik
Norwegian University of Science and Technology,
Gjøvik, Norway

Abstract. In healthcare, there are various stakeholders who hold different understandings of technology. Cybersecurity risks may also be something these stakeholder have varying perceptions of. This papers explores how cybersecurity risks are understood by two key stakeholder groups in the Norwegian healthcare sector related to welfare technology and personal healthcare devices. Two stakeholder groups (healthcare workers and technology vendors) have been interviewed to gather data on this topic. Key findings highlight that there are differences in how risks are perceived, both in terms of likelihood and in consequence. We apply risk perception theory to analyze these findings and provide suggestions for further research within this topic.

Keywords. Cybersecurity risk perception, Cybersecurity, welfare technology, healthcare technology, stakeholder perspective

1. Introduction

The healthcare sector is making use of more and more technology in their care provision, both in the in-hospital care and in remote care (e.g in nursing homes, patient's home)(Read et al. 2022; Ma et al. 2023). The need for these technologies is increasing alongside the demanding need for healthcare personnel across Europe and Asia. Making use of and implementing technology is a complex task where different people and organizations have varying acceptance criteria (Nilsen et al. 2016; Davis, 1989). Hence, people have different understandings of the world and how they make sense of it, which also affects how they understand and perceive risks in nearly all aspects of our society.
Risk perception, a field with multiple scientific viewpoints such as from psychology, sociology and engineering (Fischhoff et al., 1978;Kostyuk & Wayne, 2021; Huang et al., 2012; Sjöberg, 2000; Slovic, 1987; Slovic et al., 1982; Starr, 1969). Risk perception can be seen in light of decision making and the cognitive limitations, the structure of the environment and the uncertainty affiliated with expressing risk numerically (Gigerenzer & Todd, 1999). The individual's ability to have accessible information, and which information is available also influence risk perception (Kahneman, 2011), associated with fear or benefit (Finucane et al., 2000; Starr, 1969) and variability of different hazards (Fischhoff et al., 1978; Goh et al., 2022). The psychometric perspective views human activity and behavior and potential effects on this behavior such as context (Slovic, 1987). Another theory commonly applied to explain behavior related to risk is protection

motivation theory (PMT), where risk understanding (e.g risk perception) is explained as how individuals perceive potential danger and how dangers are coped with. Specifically, we speak of threat appraisal (perceived severity and perceived vulnerability) and the coping appraisal (response efficacy and self-efficacy) and how the individual adapts their behavior according to these (Rogers, 1983). Hence, risk perception is divided into three themes by Spencer (2016) where risk perception is influenced by mainly 1) cognitive bias, 2) social and cultural factors and 3) emotion and effect. When applying the risk perception understanding in the cybersecurity field, Huang et al. (2010) conceptualized risk perception through hazards occurring in the digital domain, and the predictors were affiliated with the severity of consequences, impact and possibility of exposure to mention a few. Another study viewed the cause-effect of the construal fit perspective to demonstrate the impact on information security risk perception (Goh et al., 2022). Cybersecurity risk perception (referred to as risk perception in the following) can be understood as the risk associated with cyber threats and the potential impact on information and communication technology (ICT) and data. This entails cyber incidents such as data breaches, hacking, malware attacks which implicate the confidentiality, integrity, availability and functionality of ICT systems and data.

In this paper, we explore how different stakeholders in the Norwegian healthcare sector perceive cybersecurity risks related to welfare technology and remote care devices. In this quest, we have limited the context to Norway and to the devices that are currently deployed in the healthcare sector, but we have not narrowed the investigation to one specific technology.

2. Method

Data can be collected in various ways, often differentiated by the qualitative and quantitative approach. We seek to explore the perception of stakeholders which requires a need to go in depth in the individual understanding and sensemaking – which is best collected through a qualitative approach. By conducting in-depth interviews, we have collected a large data material on topics relevant for cybersecurity risk perception, risk understanding and healthcare technology (welfare technology and remote care solutions) from four stakeholder groups. The inclusion criteria were:

- Needed to belong to one of the identified stakeholder groups
- Have experience with welfare technology *or* cybersecurity in the Norwegian healthcare sector

In this paper, we have included 10 interviews, with the following distribution

- Healthcare workers (N=5)
- Vendors (N=5)

The vendors included in this study deliver welfare technological services and devices widely distributed in the Norwegian healthcare system (both primary healthcare system and specialist healthcare). To preserve the anonymity of the vendors in a relatively small market, we have chosen not to disclose what type of technology they deliver. These two groups were chosen based on their opposing roles in the healthcare sector, where the healthcare workers are the ones using technology as a part of their care provision, while the vendor of technology is responsible for developing the technology that is used in this task. Albeit these two groups may be biased due to their benefit of using technology or relation to technology (e.g. as producer of technology), their opposite roles enable us to discover if there are differences in how cybersecurity risk is perceived. The interviews lasted between 45-60 minutes and were conducted through teams. All interviews have been transcribed and analyzed following the step-by-step deduction induction analysis process (Tjora, 2021). First, the data material was coded, then we reiterated the codes to catalogue codes which was finally categorized in overarching themes. The themes form the structure of the next section – results and discussion.

3. Results and discussion

In this section, we will present the key findings and discuss these in light of relevant theory. Further, we illustrate the two stakeholder groups cybersecurity risk perception to better view similarities and differences in their understanding. Cybersecurity can be expressed in various ways. One of the most common approaches is to view risk in light of likelihood (probability) and consequence (impact), and within cybersecurity this is related to the confidentiality, integrity and availability. However, in healthcare, the dimension of quality/patient safety is also highly important in thee consequence dimension (Carayon et al., 2021).

Before going into the depth of our findings, it must be noted that the two groups explored hold varying responsibility in the healthcare context. The vendors are providers of technology, used for care, whilst the healthcare workers are providing direct care for patients. Given the responses from the two stakeholder groups, it is evident that this has implication on their perception, as the vendors focus more on the business aspects and consequences if their devices were subjected to cybersecurity incidents, while the healthcare workers primary concern is the life and health of their patients. This is an interesting, and not surprising finding. However, as the vendors of technology provide equipment that is used directly in patient care, patient safety and responsibility should be a key priority. The vendors included in this study state that "Our equipment does not provide any critical tasks in the patient care, therefore we are not very concerned about the patient harm" (Vendor 1). Still, simple and basic technologies such as digital safety alarm and medicine dispenser (which are the most common in the Norwegian healthcare sector) can have potential negative consequences on patient safety. There is a mutual agreement amongst both groups that cybersecurity is important however, there were great differences on how they actually understood cybersecurity risks.

The vendors of healthcare technology have a large focus on data confidentiality i.e to ensure the privacy of data, while healthcare workers also focused on confidentiality they also cared a lot about the availability-aspect of the devices and affiliated data. When discussing risk, it is natural to explore how the two groups perceive their ability to effect and manage risk. Our respondents hold varying viewpoints in this regard, where vendors perceive the severity mainly in terms of breaches affecting confidentiality, but acknowledge the availability-aspect, such as service disruption. Healthcare workers were more concerned for the impacts for patients and their abilities to ensure patient safety, resulting in a larger focus on availability and a larger concern for related consequences. There is a shared concern for the vulnerability presented by third parties. Within coping appraisal, the vendors are aligned in their understanding, where they all believe that their strong risk management processes, in-house competence (and certifications) indicated that they have a strong coping appraisal. Risk assessments focused on CIA and patient safety (life/health) was used as an example of their self-efficacy. The healthcare workers demonstrated a low self-efficacy as they viewed cybersecurity to be the responsibility of someone else. Although, healthcare workers viewed cybersecurity as important, they also displayed limited knowledge and competence, which may implicate both perception and their self-efficacy.

Drawing on the theory of Spencer (2016) the risk perceptions of the respondents is highly influenced by especially dimension 2) Social and cultural beliefs, as there is a strong difference in their focus on business risk and consequences versus patient safety/ health risk. The primary concern of the healthcare workers is patient-focused, meaning cybersecurity incidents (intended and unintended) that can affect the care provision and safety of inhabitants, whilst the vendors focus less on this type of risk, as they also view it as highly unlikely that patients may be affected. Further, a finding that is prevalent amongst both groups is the reliance and trust placed in other parties, where healthcare workers trust and rely on the vendors for sufficient security, whilst the vendors rely on third-party providers through cloud solutions and security features such as incident detection and response. From the 10 interviews it is hard to accurately evaluate their approach to likelihood and consequence, although our findings demonstrate the healthcare workers are more concerned in terms of consequences and has less knowledge about the likelihood of cybersecurity incidents. Conversely, vendors seem less concerned about the consequences as they view the technologies deployed to be of low impact, but the dimension of data breach is viewed as likely with potential business impacts.

4. Conclusion

This study has demonstrated that there are some distinct differences in how cybersecurity risks are perceived for welfare technologies deployed in Norway amongst the two groups. Even though the two groups both view the likelihood of cybersecurity incidents to be low, there are differences in how they understand the terms and consequences of such risk. Mainly, vendors are more concerned about their business and license to operate in the healthcare sector, while healthcare workers are more concerned for the potential patient safety consequences – and they also view the consequences as more serious than the vendors. In the extension of this study, a larger number of informants should be included and one should consider conducting a tailored survey to capture the risk perception of different stakeholder groups. Another aspect that would be interesting is to examine is if there are differences between healthcare organizations, or between public/private organizations. Further, as welfare technology is a term mainly applied in the Nordics, it could be interesting to view assisted living technologies in the context of other countries than Norway to see if there are differences in how cybersecurity risks are perceived.

References

Carayon P, Wust K, Hose B, Salawei M. Human factors and Ergonomics in Health Care. In Handbook of human factors and ergonomics. 5th ed. John Wiley & Sons; 2021. p. 1417-1437.

Davis FD, Bagozzi RP, Warshaw PR. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science 1989;35:982–1003.

Finucane ML, Alhakami A, Slovic P, Johnson SM. The affect heuristic in judgments of risks and benefits. J Behav Decis Mak. 2000 Jan-Mar;13(1):1-17. doi: 10.1002/(SICI)1099-0771(200001/03)13:1<1::AID-BDM333>3.0.CO;2-S.

Fischhoff B, Slovic P, Lichtenstein S, Read S, Combs B. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy Sci. 1978;9(2):127-52. doi: 10.1007/BF00143739.

Gigerenzer G, Todd P, A.B.C. Research Group. Simple heuristics that make us smart. Oxford: Oxford University Press; 1999.

Goh ZH, Hou M, Cho H. The impact of a cause-effect elaboration procedure on information security risk perceptions: a construal fit perspective. Journal of Cyber Security. 2022;1(11). https://doi.org/10.1093/cybsec/tyab026

Huang D-L, Rau P-LP, Salvendy G, Gao F, Zhou J. Factors affecting perception of information security and their impacts on IT adoption and security practices. Int J Hum-Comput Stud. 2011 Dec;69(12):870-83. doi: 10.1016/j.ijhcs.2011.07.007.

Kahneman D. Thinking, fast and slow. London: Penguin; 2011.

Kostyuk N, Wayne C. The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. J Glob Secur Stud. 2021 Jun;6(2):ogz077. doi: 10.1093/jogss/ogz077.

Huang D, Rau P, Salvendy G. Perception of information security. Behav Inf Technol. 2010;29(3):221-32. doi: 10.1080/01449290701679361.

Ma B, Yang J, Wong FKY, Wong AKC, Ma T, Meng J, Zhao Y, Wang Y, Lu Q. Artificial intelligence in elderly healthcare: A scoping review. Ageing Res Rev. 2023;83. https://doi.org/10.1016/J.ARR.2022.101808

Nilsen ER, Dugstad J, Eide H, Gullslett MK, Eide T. Exploring resistance to implementation of welfare technology in municipal healthcare services - a longitudinal case study. BMC Health Serv Res. 2016;16:1-14. https://doi.org/10.1186/s12913-016-1913-5

Read EA, Gagnon DA, Donelle L, Ledoux K, Warner G, Hiebert B, Sharma R. Stakeholder Perspectives on In-home Passive Remote Monitoring to Support Aging in Place in the Province of New Brunswick, Canada: Rapid Qualitative Investigation. JMIR Aging. 2022;5. https://doi.org/10.2196/31486

Rogers R, Cacioppo J, Petty R. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: Unknown Conference; 1983. p. 153-77.

Sjöberg L. Factors in risk perception. Risk Anal. 2000;20(1):1-11. doi: 10.1111/0272-4332.00001.

Spencer T. Risk Perception: Theories and Approaches. New York: Nova Science Publishers, Inc.; Psychology Research Progress series

Slovic P. Perception of risk. Science. 1987 Apr;236(4799):280-5.

Slovic P, Fischhoff B, Lichtenstein S. Why study risk perception? Risk Anal. 1982;2(2):83-93. doi: 10.1111/j.1539-6924.1982.tb01369.x.

Starr C. Social benefit versus technological risk. Science. 1969 Sep;165(3899):1232-8.

Tjora A. Kvalitative forskningsmetoder i praksis. 4th ed. Oslo: Gyldendal Akademisk; 2021. 328 p.