Communicating Cybersecurity Challenges and Procuring Cybersecurity Solutions

Neshe Tuna and Ala Sarah Alaqra

Karlstad University, Universitetsgatan 2, 651 88 Karlstad, Sweden

Abstract

Cybersecurity threats are becoming increasingly sophisticated, posing severe risks to public sector, industries, and societies [1]. Addressing these threats requires innovative and collaborative strategies that leverage expertise from multiple sectors since they are too big to be faced by single organisation alone [2]. While traditional models of procurement are argued to be too complex [3], there is a growing need for agile methods that can rapidly mobilise knowledge and solutions [4].

Public sector faces challenges of articulating cybersecurity needs towards cybersecurity solution procurement. In many public organisations, this process is usually hindered by many factors, such as communication, limited collaboration among stakeholders, risk-averse culture in public buyers, and slow procurement processes [5]. Co-creation has been suggested as one way of addressing the complexity under which public organisations operate today [1].

To accelerate the response to cyber threats, we explored the use of interdisciplinary and cross-sectoral workshops (named as Challenge labs) as a means to improve cybersecurity procurement in the public sector. These workshops bring together, systematically, internal stakeholders and external experts, such as researchers and private companies (cooperations, as well as startups and SMEs), to foster better understanding, improve communication of cybersecurity requirements, and support more agile and effective procurement processes.

The Challenge lab is a structured approach to co-innovation, focusing on the earlier stages of public-private collaboration by challenge exploration with interdisciplinary and cross-sectoral participants in sandboxed workshops. Using this approach, we support the articulation of cybersecurity needs among internal and external stakeholders. This process allows the interdisciplinary discussion and communication of needs. The process creates a safe and collaborative environment where participants with diverse perspectives on cybersecurity can engage in structured dialogue. This helps bridge gaps in understanding, clarify differing risk perceptions, and surface conflicting priorities, such as between security, usability, and compliance. Interdisciplinary collaboration is crucial for aligning cybersecurity goals and co-creating realistic, actionable solutions. Our results reveal how important such processes are for communicating and articulating cybersecurity needs in private and public organisations. We will report on the procedure and share key results in this presentation.

This study is conducted within the work of the Interreg project Cross Border Cyber Growth (CBCC). CBCC aims to foster cross-border collaboration between municipalities, service providers, and innovators to improve public services and address cyber- and societal challenges that public sector faces.

References

1. Raisio, H., Puustinen, A., Valtonen, V.: Co-Creating Safety and Security?: Analyzing the Multifaceted Field of Co-Creation in Finland. International Journal of Mass Emergencies and Disasters 39(2), 263–291 (2021).
2. Clark, K., Stikvoort, D., Stofbergen, E., van den Heuvel, E.: A Dutch Approach to Cybersecurity through Participation. IEEE Security & Privacy 12(5), 27–34 (2014).
3. European Commission: Making Public Procurement Work in and for Europe. COM(2017) 572 final, Strasbourg (2017).
4. George, G., Fewer, T.J., Lazzarini, S., McGahan, A.M., Puranam, P.: Partnering for Grand Challenges: A Review of Organizational Design Considerations in Public–Private Collaborations. Journal of Management 50(1), 10–40 (2024).
5. Study on “Strategic Use of Public Procurement in Promoting Green, Social and Innovation Policies”. Final Report. European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Brussels (2015).