Chapter 56
Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda

Bilge Yigit Ozkan
https://orcid.org/0000-0001-6406-356X
Utrecht University, The Netherlands

Marco Spruit
https://orcid.org/0000-0002-9237-221X
Utrecht University, The Netherlands

ABSTRACT

There are various challenges regarding the development and use of cybersecurity standards for SMEs. In particular, SMEs need guidance in interpreting and implementing cybersecurity practices and adopting the standards to their specific needs. As an empirical study, the workshop Cybersecurity Standards: What Impacts and Gaps for SMEs was co-organized by the StandICT.eu and SMESEC Horizon 2020 projects with the aim of identifying cybersecurity standardisation needs and gaps for SMEs. The workshop participants were from key stakeholder groups that include policymakers, standards developing organisations, SME alliances, and cybersecurity organisations. This paper highlights the key discussions and outcomes of the workshop and presents the themes, current initiatives, and plans towards cybersecurity standardisation for SMEs. The findings from the workshop and multivocal literature searches were used to formulate an agenda for future research.

DOI: 10.4018/978-1-7998-7705-9.ch056

INTRODUCTION

A survey in the Global Risks Report (World Economic Forum, 2018) has revealed that cyberattacks are in the top ten risks both in terms of likelihood and impact. Cyberattacks are now seen as the third most likely global risk for the world over the next ten years. According to this study, cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Cyberattacks have both short term and long term economic impacts on different economic agents in terms of losses and expenses (Gañán, Ciere, & van Eeten, 2017).

Small and medium-sized enterprises (SMEs), which are the predominant form of enterprise and make up 99.8% of European enterprises in the Organisation for Economic Co-operation and Development (OECD) area (Digital SME Alliance, 2017), are ill-prepared for cyberattacks.

Although there is a multitude of standards available to measure, identify and improve the cybersecurity practices at organisations, many of these are not well suited for SMEs (Manso, Rekleitis, Papazafeiropoulos, & Maritsas, 2015).

In the standardisation processes, in many cases, SMEs are dependent stakeholders, and they lack resources to properly participate in the process. SMEs typically require financial support, access to technical expertise and other types of assistance to be involved in the standardisation process (de Vries, Verheul, & Willemse, 2003). In addition, SMEs may face other barriers to benefit from standards and involvement in standardisation. Awareness of standards and the process of standardisation are two important barriers (de Vries, Blind, Mangelsdorf, & Verheul, 2009).

The goal of this research is to identify the gaps (e.g. knowledge or facilitation gaps) regarding cybersecurity standardisation for SMEs by performing a literature study, analysing the trends in the literature, describing the initiatives that address SMEs, conducting an empirical study through a workshop with applicable stakeholders, and identifying opportunities for future research. Therefore, the following main research question is put forward: "What are the gaps in cybersecurity standardisation for SMEs?"

To answer this main research question in a structured way, three sub research questions were formulated. The first sub research question examines the trends in the literature and state of the art in European level initiatives addressing cybersecurity standardisation for SMEs. The second sub research question addresses the experiences and views of the stakeholders. The third sub research question addresses the future research directions to be considered to fill the gaps.

Figure 1. Main research question and sub research questions