

The Flip Side of Digitalization

Digital Ecosystems and Cybersecurity

Torben Dall Schmidt

Institute for Employment Relations and Labour

Helmut Schmidt University

tds@hsu-hh.de

Abstract

Digitalization has in the literature most often been considered from the perspective of potential social or economic benefits. This contribution considers one of the potential drawbacks of digitalisation: data and cybersecurity issues in establishments. While literature on this issue is scarce, particularly with regard to regional perspectives, it is important to gain a better understanding of the potential issues raised by digitalisation. Specifically, two mechanisms are investigated that form part of the digital ecosystem in which establishments operate. The first is the use of suppliers in digitalisation, often labelled ITOs in the literature. These suppliers are part of the digital ecosystem and may provide establishments with a cost and competence advantage in digitalisation. However, the literature also highlights potential hazards associated with using such ITOs, as this involves integrating external partners into the establishment's digital infrastructure, which increases the risk of data and cybersecurity breaches. While digitalisation may increase productivity, it may also increase the risk of major adverse shocks to production. Secondly, a small body of literature highlights the importance of technological know-how, information sharing and knowledge in mitigating such data and cybersecurity risks. It has been argued that such sharing is driven by the availability of digital infrastructure, which may depend on the location of the establishment. These are therefore aspects of the digital ecosystem of firms to consider when investigating data and cybersecurity problems.

These mechanisms associated with the digital ecosystem are investigated in terms of the likelihood of establishments experiencing data and cybersecurity problems, based on three waves of the German SOEP-LEE2 representative establishment survey for the years 2021, 2023 and 2024, comprising a total of 2519 establishments. Probability modelling is used for this analysis, including an inverse Mills ratio for selection into the final sample, taking into account selection due to item non-response in the surveys. Fixed effects are included for time, business sector, and establishment location to account for unobservable heterogeneity. The findings show that establishments that depend heavily on external partners for digitalisation are more vulnerable to data and cybersecurity problems, while high-speed local digital infrastructure in the establishment location has the opposite effect. Furthermore, high-speed local digital infrastructure that facilitates knowledge sharing mitigates the effects of external partnerships on digitalisation. This arguably point to an IV estimation strategy in support of external partners increasing likelihood of data and cybersecurity problems. The flip side of digitalization relates to such aspects of digital ecosystem.