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

Extended Abstract

Digitalization has in the literature most often been considered from the perspective of potential social or economic benefits. A focus has in particular been on productivity effects (e.g. Gal et al., 2019; Nucci et al., 2023; Anderton et al., 2023; Apostol & Hernández-Rodríquez, 2025). This contribution, however, considers one of the potential drawbacks of digitalisation: data and cybersecurity issues in establishments. Although literature on this topic is scarce, particularly with regard to regional perspectives, it is important to improve our understanding of the potential issues raised by digitalisation. Specifically, this paper investigates two mechanisms 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 form part of the digital ecosystem and can give establishments a cost and competence advantage in digitalisation. However, the literature also highlights potential hazards associated with using such ITOs, since integrating external partners into an establishment's digital infrastructure increases the risk of data and cybersecurity breaches (e.g. Benaroch, 2020; Al Harrack, 2021; Boysen et al., 2021; Topping et al., 2021; Handfield et al., 2025; Annarelli et al., 2026). While digitalisation may increase productivity, it may also increase the risk of major adverse shocks to production. Secondly, a small body of literature emphasises the importance of technological expertise, information sharing and knowledge in mitigating such data and

cybersecurity risks (e.g. Alshaikh et al., 2025). It has been argued that such sharing is driven by the availability of digital infrastructure (Marett & Xiao, 2022), which may depend on the establishment's location. These are therefore aspects of the digital ecosystem to consider when investigating data and cybersecurity issues.

The likelihood of establishments experiencing data and cybersecurity problems is investigated in terms of these mechanisms associated with the digital ecosystem, based on three repeated cross-sectional waves of the German SOEP-LEE2 representative establishment survey for the years 2021, 2023 and 2024. These were drawn from the German Federal Employment Agency's register of establishments and are stratified by size, business sector and geography (East-West Germany). A total of 2,519 establishments were included in the survey. Probability modelling is employed in this analysis, incorporating an inverse Mills ratio to account for selection into the final sample and for item non-response in the surveys. This is based on the characteristics of the respondent within the organisation, which are largely available for the critical item non-response for the establishment variables considered here. Specifically, probit models are first used to investigate which establishment characteristics are important for using external partners for digitalisation in relation to the likelihood of data and cybersecurity problems. The findings show that external partnerships increase the likelihood. However, this may be confounded by the number of digital technologies used by the establishments, as the use of more digital technologies may be related to the use of external partnerships. Accordingly, a count variable is included to control for the use of different technologies (customised software, data analytics, big data, robots, virtual/augmented reality, AI and 3D printing). The effects of external partnerships remain robust. Furthermore, the use of internal resources within establishments for data and cybersecurity issues may affect the impact of external partnerships by mitigating the integration of external partners into an establishment's internal digital solutions. The findings do not support this; rather, internal staffing relating to data and cybersecurity problems is related to the number of digital technologies. Dependence on external partners for digitalisation appears to lead to integration into the establishment's internal

digital solutions, making it vulnerable regardless of internal resources or digital complexity. These establishment-specific results control for fixed effects over time and business sectors.

A regional perspective is added by considering the availability of digital infrastructure at the location of the establishment. To achieve this, the digital infrastructure in a firm's location is matched to the establishment by NUTS3 levels. This digital infrastructure data is obtained from the Broadband Atlas of the German Federal Ministry of Digital Affairs and Transport (BMDV). The focus is on fixed-link broadband, which has two quality characteristics in the statistics: The first is the proportion of establishments covered by NUTS3, and the second is the connection speed. Continuous variables for coverage at a given speed are included as independent variables in previous models, while also adding fixed effects for establishment location by NUTS3, in addition to fixed effects for time and business sector. It is found that higher coverage of speeds of at least 200 Mbps reduces the likelihood of data and cybersecurity problems in establishments. Following the literature, this may be interpreted as resulting from better technological know-how and information sharing facilitated by high-speed broadband. While the addition of both external partnerships and fixed-line broadband coverage provides insight into the impact of digital ecosystems on the likelihood of data and cybersecurity issues, it does not reveal whether fixed-line broadband has a direct impact on this likelihood or whether it moderates the impact of external partners. To this end, models that include interaction terms for both factors are used to investigate such conditional effects. Although interaction effects are difficult to handle in a probit model, models incorporating such interactions are used to produce margin plots illustrating the likelihood of external partnerships relating to data and cybersecurity problems in relation to broadband coverage at a given speed level. The results show that the moderating effects of strong dependence on external partners in digitalisation are particularly significant for broadband connections of 1000 Mbps or more, and that the probability of a cybersecurity problem arising from a partnership decreases with higher coverage.

One concern regarding these results is reverse causality. For example, does the strong dependence on external partners for digitalisation increase the likelihood of data and cybersecurity problems arising from their integration into the establishment's internal digital solutions, or does the occurrence of such problems lead establishments to turn to external partners for digitalisation assistance? This is clearly a concern. While it may be debatable whether local digital infrastructure, in terms of broadband coverage at the establishment's location, is also a consequence of the establishment having experienced data and cybersecurity problems, it should be noted that, in the estimations with interactions between broadband coverage and external partners, the effect of broadband coverage seems to run through external partners, but does not have a significant direct effect on data and cybersecurity problems. This may be an initial indication that local broadband coverage satisfies the exclusion restriction in IV estimation. Secondly, the relevance criterion may also be met. While the arguments on information sharing and technological know-how were general and not conditional on using external partners, local high-speed broadband coverage may indeed be important given the strong dependence on external partnerships for digitalisation. This is because integrating external partners into the establishment of internal digital solutions and structures may only work effectively in the presence of strong local digital infrastructures. The importance of digital ecosystems clearly has a local dimension. Using local fixed-link broadband coverage of 1000 Mbps or more as a means of achieving a high level of digitalisation with external partners points to robust results in terms of the increased likelihood of data and cybersecurity problems with these partners. However, aspects of digital ecosystems may mitigate the risks associated with a strong dependence on external partners for digitalisation, thereby reducing the likelihood of data and cybersecurity problems. In this way, such local digital infrastructures are important in reducing risks and increasing cost and productivity benefits from using external partners for digitalisation. This has clear policy implications for the construction of such local digital infrastructures.

References

Al Harrack, M. (2021). Cybersecurity Risks in Outsourcing Strategies. *Academia Letters*, November 2021, 1-6. https://doi.org/10.20935/AL4161.

Alshaikh, M., Mehmood, S., Amin., R. & Alsubaei, F.S. (2025). The Impact of Cybersecurity Through Knowledge Sharing Practices: Limitations, Analysis of Current Trends and Future Research Directions. *International Journal of Advanced Computer Science and Applications (IJACSA)* 16 (3), 1007-1029. http://dx.doi.org/10.14569/IJACSA.2025.0160398.

Annarelli, A., Colabianchi, S., Nonino, F., Oropallo, E. & Palombi, G. (2026). Is cybersecurity outsourcing always effective? Strategic organisational insights and knowledge in the era of digitalization. *Journal of Innovation & Knowledge*, 14, 100939, https://doi.org/10.1016/j.jik.2026.100939.'

Anderton, B., Botelho, V. & Reimers, P. (2023). Digitalisation and productivity: Gamechanger or sideshow? ECB Working Paper No. 2794. European Central Bank (ECB), Frankfurt a. M.

Apostol, S., & Hernández-Rodríguez, E. (2025). Digitalisation in European regions: unravelling the impact of relatedness and complexity on digital technology adoption and productivity growth. *Industry and Innovation*, 32(7), 772–801. https://doi.org/10.1080/13662716.2024.2423731.

Benaroch, M. (2020). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. In: Hirschheim, R., Heinzl, A., Dibbern, J. (eds) *Information Systems Outsourcing. Progress in IS*. Springer, Cham. https://doi.org/10.1007/978-3-030-45819-5_13.

Boyens, J., Paulsen, C., Bartol, N., Winkler, K. & Gimbi, J. (2021). Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. NIST IR 8276, National Institute of Standards and Technology, US Department of Commerce. https://doi.org/10.6028/NIST.IR.8276.

Gal, P., Nicoletti, G., von Rüden, C. & Sorbe, S. (2019). Digitalization and Productivity: In Search of the Holy Grail - Firm-level Empirical Evidence from European Countries. *International Productivity Monitor*, Centre for the Study of Living Standards, 37, 39-71.

Handfield, R., Earp, J. & Sadeghi, A.H. (2025). Reducing cybersecurity vulnerabilities in the supply base: Insights from cyber experts. *Technology in Society*, 82, 102947. https://doi.org/10.1016/j.techsoc.2025.102947.

Marett, K. & Xiao, S. (2022). Broadband Internet Access as a Localized Resource for Facilitating Information Security Knowledge. Journal of Midwest Association of Information Systems, 2022 (1), 8-22. https://aisel.aisnet.org/jmwais/vol2022/iss1/2.

Nucci, F., Puccioni & C., Ricchi, O. (2023). Digital technologies and productivity: A firm-level investigation. Economic Modelling, 128, 106524. https://doi.org/10.1016/j.econmod.2023.106524.

Topping, C., Dwyer, A., Michalec, O., Craggs, B. & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 108, 102324, https://doi.org/10.1016/j.cose.2021.102324.