Author: Sebastian Steffen (2022)

Committee: Erik Brynjolfsson (chair), John Horton, Sinan Aral, Prasanna Tambe (The Wharton School, University of Pennsylvania)

Abstract:

This dissertation contains three essays concerning the economics of information technology, human capital, and the future of work. In the first essay, 'Occupational Change: Automation and Reskilling Risks', I develop a methodology to study occupational skill demands and estimate the returns to skills, by leveraging novel data from over 200 million online job postings from 2010 until 2020. I find large heterogeneity in skill returns across industries and identify potential (re)skill investment opportunities for workers. In the second essay, 'Digital Resilience: How Work-From-Home Feasibility Affects Firm Performance', I build on the methodology and data from the previous chapter to measure how feasible it is for firms to shift their workforce to remote work. Using these data, I then causally identify how much remote work practices aided firms' resilience against the Covid-19 pandemic, as measures by sales, net income, stock market returns, and volatility. The findings highlight that firms need to strategically manage the labor composition and digitization of their organizations, and consider that work-from-home practices, besides their many other advantages, are an effective way to hedge against operational risks. In the final essay, 'Treating the Symptoms or the Cause? Substantive and Symbolic Talent Acquisition in Response to Data Breaches', I use the data from the first chapter to study firms' hiring responses to data breaches. Advancing the theory of substantive and symbolic IT adoption to complementary human capital acquisitions, I find that firms significantly increase their hiring for cybersecurity as well as public relations and legal workers after suffering breach. I also find that public scrutiny can serve as an effective mechanism to shift firms' hiring investments toward substantive, rather than symbolic measures. Given the increase in the volume and severity of cyberattacks, these results provide important and timely insights into firms' responses and incentives to more substantively safeguard their data.