Abstract

Cybersecurity has emerged as one of the most pressing global concerns, as the expansion of attack surfaces and the growing sophistication of cyber threats, such as phishing and social engineering, increasingly threaten the resilience of individuals, organizations, and societies alike. This dissertation addresses the challenges of organizational cybersecurity in the new reality of knowledge work, a reality shaped by rapid technological advancements, changing employee behaviors, and organizational shifts toward flexible work models. While prior research has predominantly focused on technological solutions, this dissertation argues for a more holistic approach that integrates human, organizational, and technological dimensions to effectively address cybersecurity challenges. To navigate the complex cybersecurity challenges and provide a comprehensive perspective, the dissertation adopts a cumulative approach, consisting of three research projects, and employs methodological pluralism by combining both quantitative and qualitative methods. The first project aims to develop a typology of employee cybersecurity behaviors based on an online survey and cluster analysis. The resulting typology distinguishes four archetypes of knowledge workers with different cybersecurity attitudes and behaviors, highlighting the need for tailored cybersecurity interventions that account for individual differences. The second project focuses on phishing detection behavior and examine effects of visual risk indicators embedded in email interfaces on employees' decision-making processes. The results of an eye-tracking lab experiment indicate that visual cues can improve phishing detection, emphasizing the relevance of human-technology interactions. The third project examines the impact of flexible work arrangements on organizational cybersecurity, using a three-dimensional framework to conceptualize work flexibility and insights from expert interviews. The findings reveal that flexible work arrangements introduce multifaceted cybersecurity risks, requiring comprehensive countermeasures that align with broader organizational needs, such as employee autonomy. Collectively, this dissertation advances the understanding of cybersecurity by recognizing the need to move beyond rather singular human, technological, or organizational perspectives. Beyond theoretical contributions to cybersecurity and information systems research, it provides actionable recommendations for organizations to develop informed cybersecurity strategies. By acknowledging human variability, technological advances, and organizational changes, the dissertation contributes to a more comprehensive understanding of cybersecurity in organizational contexts.

Key words: *Cybersecurity, Phishing, Knowledge worker behavior, User typology, Cluster analysis, Human-computer interaction, Eye-tracking, Visual risk indicators, Flexible work, Remote work, Value destruction, Reactance Theory*

Zusammenfassung

Die Cybersicherheit hat sich zu einem der drängendsten globalen Probleme entwickelt, da die Ausdehnung der Angriffsflächen und die zunehmende Ausgereiftheit von Cyber-Bedrohungen wie Phishing und Social Engineering die Widerstandsfähigkeit von Einzel-personen, Organisationen und Gesellschaften gleichermaßen bedrohen. Diese Dissertation befasst sich mit den Herausforderungen der organisatorischen Cybersicherheit in der neuen Realität der Wissensarbeit, einer Realität, die durch rasche technologische Entwicklungen, veränderte Verhaltensweisen der Mitarbeiter und organisatorische Veränderungen hin zu flexiblen Arbeitsmodellen geprägt ist. Während sich die bisherige Forschung vorwiegend auf technologische Lösungen konzentriert hat, plädiert diese Dissertation für einen ganzheitlich-eren Ansatz, der menschliche, organisatorische und technologische Dimensionen integriert, um die Herausforderungen der Cybersicherheit effektiv anzugehen. Um die komplexen Herausforderungen im Bereich der Cybersicherheit zu bewältigen und eine umfassende Perspektive zu bieten, verfolgt die Dissertation einen kumulativen Ansatz, der aus drei Forschungsprojekten besteht, und setzt auf methodischen Pluralismus, indem sie sowohl quantitative als auch qualitative Methoden kombiniert. Das erste Projekt zielt darauf ab, auf der Grundlage einer Online-Umfrage und einer Clusteranalyse eine Typologie des Cyber-sicherheit-Verhaltens von Mitarbeitern zu entwickeln. Die sich daraus ergebende Typologie unterscheidet vier Archetypen von Wissensarbeitern mit unterschiedlichen Einstellungen und Verhaltensweisen hinsichtlich Cybersicherheit, was den Bedarf an maßgeschneiderten Cybersicherheitsmaßnahmen unterstreicht, welche individuelle Unterschiede berücksich-tigen. Das zweite Projekt konzentriert sich auf das Phishing-Erkennungsverhalten und untersucht die Auswirkungen visueller Risikoindikatoren, die in E-Mail-Benutzeroberflächen eingebettet sind, auf die Entscheidungsprozesse der Mitarbeiter. Die Ergebnisse eines Eye-Tracking-Laborexperiments deuten darauf hin, dass visuelle Hinweise die Phishing-Erken-nung verbessern können, was die Bedeutung der Interaktion zwischen Mensch und Technik unterstreicht. Das dritte Projekt untersucht die Auswirkungen flexibler Arbeitsregelungen auf die Cybersicherheit in Unternehmen, wobei ein dreidimensionaler Rahmen zur Konzeptu-alisierung von Arbeitsflexibilität und Erkenntnisse aus Experteninterviews verwendet werden. Die Ergebnisse zeigen, dass flexible Arbeitsregelungen vielfältige Risiken für die Cybersicherheit mit sich bringen und umfassende Gegenmaßnahmen erfordern, die mit den allgemeinen organisatorischen Anforderungen wie Mitarbeiterautonomie in Einklang stehen müssen. Insgesamt trägt diese Dissertation zu einem besseren Verständnis der Cyber-sicherheit bei, indem die Notwendigkeit anerkennt wird, über eine eher singuläre mensch-liche, technologische oder organisatorische Perspektive hinauszugehen. Neben theoretischen Beiträgen zur Cybersicherheits- und Informationssystemforschung werden umsetzbare Empfehlungen für Unternehmen zur Entwicklung fundierter Cybersicherheitsstrategien gegeben. Durch die Berücksichtigung menschlicher Variabilität, technologischer Fortschritte und organisatorischer Veränderungen trägt die Dissertation zu einem umfassenden Verständnis der Cybersicherheit im organisatorischen Kontext bei.

Schlüsselwörter: *Cybersicherheit, Phishing, Wissensarbeiter-Verhalten, Benutzer-typologie, Clusteranalyse, Mensch-Computer-Interaktion, Eye-Tracking, Visuelle Risiko-indikatoren, Flexible Arbeit, Fernarbeit, Wertvernichtung, Reaktanztheorie*