6-14-2024

Compartmentalization Vs Integration: Tensions Between Digital Security Innovations and Security Governance

Niki Panteli
Lancaster University, n.panteli1@lancaster.ac.uk

Tonii Leach
Royal Holloway University of London, antonia.leach@rhul.ac.uk

Lizzie Coles-Kemp
Royal Holloway University of London, lizzie.coles-kemp@rhul.ac.uk

COMPARTMENTALIZATION VS INTEGRATION: TENSIONS BETWEEN DIGITAL SECURITY INNOVATIONS AND SECURITY GOVERNANCE

TREO Paper

Niki Panteli, Lancaster University, Lancaster, UK, n.panteli1@lancaster.ac.uk

Antonia Leach, Royal Holloway University of London, Egham, UK, antonia.leach@rhul.ac.uk

Lizzie Coles-Kemp, Royal Holloway University of London, Egham, UK,

lizzie.coles-kemp@rhul.ac.uk

Abstract

The paper presents an emerging idea that centres around digital security innovations in organizations. In particular, the study, which is still at an early stage, seeks to explore how digital security innovations affect security governance. Though there is a growing literature on the importance and role of security governance, little is known about how this may need to be reconfigured because of digital security innovations. In this exploratory qualitative study, we examine possible tensions that may arise between security innovations and security governance and explore ways for resolving these. The study draws on the use of a specific security innovation with compartmentalised features.

Keywords: digital security innovations, security governance, tensions, CISOs, qualitative methods

1 Introduction

A significant body of literature exists on the increased necessity for organizations to develop robust and resilient security systems, especially in the current climate of cyberattacks and cyber vulnerabilities. Despite this recognition, there has been to-date limited exploration of the impact of security innovations on digital security governance.

Similar to other organizational functions with an evolving technology landscape, security needs new investments in technology in order to deal with the increased risks, threats and vulnerabilities. As part of the growing need to develop robust security systems, it is important to understand the impact of these innovations on those who govern such systems, including the potential tensions that may be created between innovations on the one and governance on the other. Following this, the driving question of the study is: *What tensions may arise between digital security innovations and digital security governance and how can these be managed?*

2. Conceptual Foundations

2.1 Tensions at times of change

Tensions, especially those that are paradoxical in nature, are prominent within the organizational context with literature seeking to understand how opposing or contradictory alternatives may be managed (e.g. Koukouvinou et al. 2023). Research on technological change in organizations has found several tensions which may arise, such as control and flexibility (Svahn et al. 2017), whilst within the innovation literature, there has been reference to tensions in relation to exploration and exploitation (Smith and

Lewis, 2011). Within security management research, Raza et al. (2018) found that paradoxical tensions exist between digital innovation and information security compliance, with the one promoting flexibility and the other promoting stability, and therefore representing competing demands for organizations.

2.2 Digital Security Governance

Digital security governance refers to the management and control of security systems comprising of technology and people, as well as organizational factors such as structures, processes and standards (Schinagl et al. 2022). In recent years there has been a growing recognition that human and organizational factors matter in security governance. Existing research has pointed to the important role of information security leaders or CISOs as well as the role of corporate governance and the board of directors - particularly in information security (Gale et al., 2022). Studies in this area posit that security is more an administrative, rather than technological innovation (Hsu et al. 2012). As Hsu et al. (2012) explain, whereas technological innovations are about the development of security technologies, information security from an administrative innovation perspective is about "the development of a security management program including the security policy, management committee, team structure (e.g., CISO or security officers), risk-management process, and employee education to preserve the confidentiality, integrity, and availability of information in organizations" (p.920). This broader perspective of security aligns with Wallace, Green et. al. (2021) who argue that traditional technology adoption frameworks such as Technology Organization Environment (TOE) framework, do not sufficiently capture the range of issues that security faces. The researchers instead proposed an extended framework that encompasses new dimensions, including cyber catalysts such as risks, privacy and vulnerabilities, and practice standards which include ethics, insurance, legal and assessment. We concur with this view that the security context is different to other technology adoption contexts and that human and organizational factors play a key role in developing robust and resilient security management.

It is within this broader context that we aim to understand tensions that may arise because of new digital security systems and technology innovations within this domain. In what follows, we present an exemplar digital security innovation upon which this study is centred on, and following this we present the research design adopted.

3. CHERI - Digital Security Innovation

In the present study, we draw on our own engagement with an interdisciplinary and cross-sectoral research project on a specific innovation in digital security. This engagement derives from our work as part of the UKRI-funded Discribe Hub+, a multi-institutional and cross-disciplinary social scientific research programme dedicated to understanding the societal, economic, and political implications of innovation in digital security technology. The Discribe Hub+ is a subsidiary of a wider programme of innovation between the UK government, academia and the private sector called Digital Security by Design (DSbD). The primary objective of DSbD is to facilitate the adoption of an 'on chip' hardware security model for memory protection and compartmentalisation developed by computer science researchers at the University of Cambridge called CHERI (Watson et al. 2015). This technological innovation offers the potential to robustly control access to data by compartmentalising malware and thereby stopping its spread and by implementing granular data protection profiles.

4. Design and Methodology

The study is exploratory and draws on the qualitative research design approach. Data collection (which is still under way) is based on a series of semi-structured interviews with cybersecurity leaders and other experts within the DSbD network. This is important as we are seeking to interview people who had knowledge of DSbD, and CHERI in particular. CHERI has been used in our study as an exemplar of a digital security development in order to encourage exploration of ideas about how innovations in cybersecurity may affect security governance. Within the semi-structured interviews, we ask participants to share their organization's security governance context. Following this, we present them with a short scenario related to CHERI and then ask about the potential impact of this on the security

governance of the organization and any possible tensions that may arise. All interviews are conducted via MS Teams, recorded, and transcribed.

5. Tentative implications

Tentative findings of the study so far, based on a selected number of interviews, indicate a tension between compartmentalization, which is a key feature of the digital security innovation studied, and the need for integration for security governance purposes. We consider this tension important as it has implications on the adoption, implementation and sustenance of the digital security innovation. Another tension exists between the need for agility and the locking in effect following the move to the new digital security systems; the latter requiring new hardware, software and technical skills. In the next stages, we will be exploring this tension further. The study is expected to contribute to the field of digital security governance by identifying effective ways through which security governance can be reconfigured to support much needed digital security innovations. Though tensions can be seen as disruptive in the innovation process, they can also serve as effective mechanisms if they are managed appropriately. We expect the findings of this study to shed light in this direction.

Acknowledgements

Funded by ESRC DiscribeHub+ ES/V003666/1.

References

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840.

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information systems research*, *23*(3-part-2), 918-939.

Koukouvinou, P., Simbi, N., & Holmström, J. (2023). Managing unbounded digital transformation: exploring the role of tensions in a digital transformation initiative in the forestry industry. *Information Technology & People*, *36*(8), 43-68.

Raza, H., Baptista, J., & Constantinides, P. (2018). Paradoxical tensions between digital innovation and information security compliance in a large financial services organization. In *The 34th EGOS Colloquium*.

Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers & Security*, *122*, 102903.

Smith, W. K., & Lewis, M. W. (2011). Toward a theory of paradox: A dynamic equilibrium model of organizing. *Academy of management Review*, 36(2), 381-403.

Svahn, F., Mathiassen, L., & Lindgren, R. (2017). Embracing digital innovation in incumbent firms. *MIS Quarterly*, 41(1), 239-254.

Wallace, S., Green, K., Johnson, C., Cooper, J., & Gilstrap, C. (2021). An Extended TOE Framework for Cybersecurity Adoption Decisions. *Communications of the Association for Information Systems*, *47*(2020), 51.

Watson, R. N., Woodruff, J., Neumann, P. G., Moore, S. W., Anderson, J., Chisnall, D., ... & Vadera, M. (2015, May). CHERI: A hybrid capability-system architecture for scalable software compartmentalization. In *2015 IEEE Symposium on Security and Privacy* (pp. 20-37). IEEE.