Guest Editorial Preface

Special Issue on Managing Information Security Risks in Digital Business

Xin (Robert) Luo, University of New Mexico, USA
Carol Hsu, Tongji University, China
Dionysios Demetis, University of Hull, UK

The transition from computer security to information security and the higher degree of interconnectivity afforded by new technologies like the Internet of Things have progressively created more complex and more open ecosystems. In our call for papers, we requested contributions that view the management of information security risks as a key pillar for the organizational resilience of digital businesses. In this context, we were interested in understanding how organizations or individuals can effectively mitigate the cybersecurity risks for digital businesses and how organizations can develop digital security strategies in today's technology-based world. Thus, we requested submissions that focus on the interplay of technical, behavioral, economic and/or organizational perspectives on information security.

We are grateful for all the interest in our special issue and in the variety of submissions we have received. Ultimately, two papers were selected for the special issue.

In the first paper entitled "The Differential Effects of Interpersonal Justice and Injustice on Computer Abuse: A Regulatory Focus Theory Perspective," the authors examined the emotional and behavioral reactions to employees' experiences of interpersonal injustice based on regulatory focus theory. The results of the paper demonstrate that employees experience more hostility in reactions to perceptions of interpersonal injustice and that employees' personalities moderate the relationship between the emotions experienced and computer abuse. In this context, the contribution of the authors informs the broader spectrum of behavioural IS research in cybersecurity. The authors highlight the need to distinguish the effects of other justice, such as procedural justice/injustice and distributive justice/injustice, from other emotional reactions under a cybersecurity context. They show that emotions play an important role in explaining the relationship between justice and computer abuse. They also find that individual personalities, specifically those that maintain a promotion focus or a prevention focus, influence the effect of emotions on computer abuse. This stresses the pressing need to consider the role of personalities when analysing the effect of emotions; individuals may experience the same emotion when facing unfair treatment from supervisors, but individuals with different personalities will have different behavioral reactions. Both insider threats research and the broader behavioral streams of IS security research can be informed by these results.

At the same time, the paper highlights a few important practical contributions: a) managers should make efforts to improve employees' perception of their own ideals regarding the self in order to increase their citizenship behaviors, b) when attempting to avoid threats, employees are more likely to experience hostility so managers should consider the presence of an appropriate stimulus when interacting with employees in order to mitigate negative emotions and enhance positive emotions, c) managers should select different treatment strategies when interacting with different employees.

In the second paper entitled "It's Not My Fault: The Transfer of Information Security Breach Information," the authors attempt to understand the dynamics of the transfer of information security breach information by examining 1) whether such an effect exists at the intra-industry level or at the competitor level and 2) how the transfer of information security breaches information can vary by cause and type of information compromised. Their results suggest that the effect of the transfer of information security breach information occurs only among major competitors with similar products. This has a number of implications: first, managers need to be more aware of any potential information security breaches faced by their rivals as the effect of the transfer of information security breach information arises only among major competitors with similar products, but this can lead to varying outcomes. Second, prioritization of control/prevention mechanisms needs to be based on different scenarios. While the authors are the first to acknowledge limitations of this work (e.g. difficulty in data limitations, capture all possible factors, etc.), their work underscores the importance of looking at broader information transfer effects in cybersecurity, mostly within an industry but also explore any other effects between industries. Overall, their work illustrates that the actual impacts of security breaches have more complex side-effects, including the way rivals 're-engineer' their own security approaches and how customer decisions to move to a different provider of a product or a service may affect these dynamics.

Together, these papers provide an excellent opportunity to consider more subtle forms in the interplay between technical, behavioral, economic and/or other organizational perspectives on information security. The systemic interpenetration of organizational dynamics, enabled by a digital fabric that transcends silos and boundaries, present new challenges for information security. We are excited to see these papers in our issue and hope that novel approaches of exploring these problems emerge from their contributions.

Xin Luo
Carol Hsu
Dionysios Demetis
Guest Editors
JDM