Introduction to the HICSS-58 Minitrack on Innovative Behavioral IS Security and Privacy Research

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Karen Renaud
University of Strathclyde
karen.renaud@strath.ac.uk

Anthony Vance
Virginia Tech
anthony@vance.name

Allen C. Johnston
University of Alabama
ajohnston@cba.ua.edu

This minitrack provides a venue for innovative research that rigorously addresses the risks to information system security and privacy, with a specific focus on individual behaviors within this nomological net. Domains include work related to detecting, mitigating, and preventing both internal and external human threats to organizational security. Papers may include theory development, empirical studies (both quantitative and qualitative), case studies, and other high-quality research manuscripts, with a particular interest in emerging, rigorous research methods for investigating their phenomenon of interest.

This year's minitrack features two sessions. The first session focuses on **Threats and AI** and includes three papers that will stimulate further discussion and exploration of the key phenomena within this domain. The first paper in this session is one by Danylak, Lins and Sunyaev titled: "*The Role of Employees' Threat Appraisal in Security Certification Compliance: Insights from a Protection Motivation Approach."* This study examines how employees' threat appraisals influence their compliance with security certification requirements, particularly ISO/IEC 27001, using Protection Motivation Theory (PMT) as a framework. It finds that perceived security threats and compliance costs significantly impact employees' certification compliance intentions, with fear increasing compliance motivation, while the perceived threat of customer loss surprisingly reduces compliance intention.

The first session's second paper, titled "*You've been Phished! The Effect of Threat Susceptibility in Fear Appeal Messages on Employee Security Training Motivation and Learning*" by Shuraida, investigates the impact of fear appeal messages with varying levels of threat susceptibility on employees' motivation to participate in information security training and their protective behaviors. Results show that employees exposed to high threat susceptibility messages were more likely to complete the training and, after training, were less likely to fall victim to a phishing attack compared to those who received low susceptibility messages.

The third paper in the first session is one by Frank, Brennecke, Hölzmer, Pocher and Fridgen, titled "Potential of AI for Human-Centric Cybersecurity in the Financial Sector." This paper explores the potential of AI-powered, human-centric cybersecurity measures in the financial sector, focusing on how AI can enhance the workforce's ability to combat cyber threats. Through a structured literature review and a Delphi study, it identifies promising AI-enhanced cybersecurity solutions that can support financial institutions by equipping their employees with tools and training to effectively respond to evolving cyberattacks.

The second session of their year's minitrack focuses on **Security & Privacy Behavior**. It includes four papers that promise to incite reflection and discussion on a number of important research topics and outcomes. The first paper in the second session is by Prabhu and Dell titled "*The Nexus Between Sanctions and Neutralization in Information Security.*" This paper investigates how sanctions and neutralization techniques interact to shape employees' intentions to comply with information security policies, focusing on behaviors like using removable storage devices and opening unsafe links. It finds that while neutralization weakens the effect of sanctions on compliance, stringent sanctions can mitigate this impact, suggesting that organizations should enforce strong penalties to counterbalance employees' tendency to justify non-compliant behaviors.

The second paper of the second session is by Reittinger and Pernul titled "A Taxonomy of Positive Incentives to Motivate Cybersecurity Behaviors." This paper presents a taxonomy of incentives for employees security behaviors, so as to align employees' interests with those of organizations. The taxonomy, consisting of 5 dimensions and 32 characteristics, was validated by a panel of industry experts. The authors also provide an

URI: https://hdl.handle.net/10125/109386
978-0-9981331-8-8

interactive, open source tool to facilitate use of the taxonomy.

The third paper of the second session is by Keith, Giboney and LeVasseur titled "*Mandated Information Disclosure Theory: Understanding Information Privacy and Disclosure Decisions in Educational Technology (EdTech).*" This paper develops the mandated information disclosure theory (MIDT) which explains privacy and disclosure decisions in the context of educational technology (EdTech). The context of the EdTech industry is unique in that students bear the risk of information disclosure through the use of EdTech tools, but have little-to-no control on EdTech adoption decisions. Therefore, traditional utility models of disclosure do not apply. The authors present process and variance versions of MIDT that provide understanding of privacy issues in the EdTech sector.

The fourth paper of the second session is by Luu, Harrison, Samuel and Jones, titled "*Proposing A Unified Concept of Information Privacy: An Actor/Action-Oriented Approach.*" This paper introduces a unified, actor/action-oriented concept of information privacy that emphasizes the need to address privacy concerns in the context of rapidly evolving technologies, such as AI and data inference practices. It proposes a multilevel framework that integrates various actors (e.g., individuals, institutions, regulatory systems) and actions (e.g., data collection, management, and analysis) to better capture the dynamic and multifaceted nature of information privacy in today's digital landscape.