

## Introduction to the HICSS-56 Minitrack on Innovative Behavioral IS Security and Privacy Research

Merrill Warkentin  
Mississippi State University  
[m.warkentin@msstate.edu](mailto:m.warkentin@msstate.edu)

Anthony Vance  
Virginia Tech  
[anthony@vance.name](mailto:anthony@vance.name)

Allen C. Johnston  
University of Alabama  
[ajohnston@cba.ua.edu](mailto: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 security policy compliance 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 Mattson, Aurigemma, and Ren titled, "Close the Intention-Behavior Gap via Attitudes: Case Study of the Volitional Adoption of a Two-Factor Authentication Service." In this study, the authors explore the intention-behavior gap that has long perplexed scholars. Through their exploration, the authors point to negative attitudes toward different functional areas as a key facilitator of this gap and suggest it the negative attitudes must change if the gap is to be mitigated.

The first session's second paper, titled "Buying in and Feeling Responsible: A Model of Extra-role Security Behavior" by Nehme and Marler, contributes to the discussion of the value of extra-role security behaviors to information security practices by examining the important role "felt responsibility for constructive change" (FRCC) has in driving extra-role security behavior and how a user's proactive personality can help drive their sense of FRCC when they

participate in information security policy-related activities.

The third paper in the first session is one by Cram and D'Arcy, titled "Barking Up the Wrong Tree? Reconsidering Policy Compliance as a Dependent Variable within Behavioral Cybersecurity Research." In this paper, the authors examine the limitations associated with using cybersecurity policy compliance as a dependent variable and challenge scholars to continue to refine cybersecurity research by adopting an increasingly risk-centric approach that focuses on insecure cybersecurity behavior, cybersecurity vulnerabilities, and actual incidents.

The second session of their year's minitrack focuses on information privacy and social learning research. It includes two 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 Ahmad, Gal, and Liu titled "Design of Surveillance Technologies and Privacy Concern." Based on a review of 207 prominent information technology (IT) journals, the authors determine that both non-obtrusive and obtrusive surveillance are used at individual, corporate and societal level differentially. The authors proceed to suggest new areas of future research that promise to enrich academic discourse in IS and create value for corporate firms, government and policy makers.

The second and final paper of the second session is by Hengstler, Kuehnel, and Trang titled "Is Social Learning Always Helpful? Using Quantile Regression to Examine the Impact of Social Learning on Information Security Policy Compliance Behavior." Through the use of quantile regression, the authors estimate the overall impact of social learning interventions on ISP compliance behavior across

three categories of employees: employees who tend to behave in an ISP non-compliant manner, employees with average compliance behavior, and employees who tend to behave in a rather strict ISP compliant manner. The findings of this research support the notion that the impact of social learning interventions differs across employees with different propensities for information security policy compliance behavior; thus motivating scholars to consider quantile regression and social learning social learning theory when analyzing compliance behavior in their future research.