Introduction to the HICSS-57 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 three sessions. The first session focuses on **Behavioral Cyber Security** 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 Phillips, Aurigemma and Brummel titled: "*Leveraging Situational Judgment Tests to Measure Behavioral Information Security."* This study introduces the Situational Judgement Test (SJT) to cybersecurity research as a means of measuring security behaviors. Like the scenario and factorial survey methods before it, the SJT has potential to yield important insights into security behaviors and individuals' rationales behind their behaviors. SJTs are instruments that present a scenario along with several items that measure multiple constructs. Thus, SJTs are multidimensional instruments that situate measures within a described context that excel in measuring typical or maximal performance of individuals. SJTs ensure that the instrument fits a particular organization context or environment belonging to the sample frame. The authors demonstrate why SJTs are a valuable measurement technique for IS security researchers to consider.

The first session's second paper, titled "*Stage Theorizing in Behavioral Information Systems Security Research*" by Siponen, introduces the concept of stage modeling as an alternative to variance and process models in IS and ISS literature. The authors argue that stage models are a good choice when the phenomenon of interest is not best captured by a change or development resulting from a sequence of events. They also argue that the goals of the scientific modeling are important in deciding the characteristics a stage model should have.

The third paper in the first session is one by Schaltegger, Ambuehl, Ackermann and Ebert, titled "*Re-thinking Decision-Making in Cybersecurity: Leveraging Cognitive Heuristics in Situations of Uncertainty.*" This paper argues that heuristics, or simple rules of thumb, can be used to improve cybersecurity by making decision-making more adaptive and economical. The authors point out that heuristics have been successfully used in other domains, such as medical diagnosis and financial trading, and that these domains share similarities with cybersecurity, such as uncertainty and time pressure. The authors argue that heuristics should not be dismissed out of hand, but that further empirical research is needed to determine the specific environments where heuristics are advantageous for cybersecurity. They suggest that heuristics could be particularly useful in phishing detection and incident response, where speed and accuracy are essential.

The second session of their year's minitrack focuses on **Information Privacy - Disclosure and Consent**. It includes three 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 Miltgen, Crossler and Mahid titled "*Holistic or Analytic: Does it Matter How Intention to Disclose Information is Measured?*" This paper studies the differences between holistic and analytic approaches to measuring people's intentions to disclose information and how they affect the understanding of what factors lead to information disclosure. The paper proposes a new model for understanding how people make decisions about disclosing personal information. The authors found that measuring disclosure decisions analytically is a more precise way to capture disclosure intentions.

URI: https://hdl.handle.net/10125/106950
978-0-9981331-7-1

The second paper of the second session is by Tjostheim titled "*Exploring Data-Disclosure Vulnerabilities and Phishing Assessed by the Cognitive Reflection Test*." This paper investigates the factors that contribute to phishing susceptibility. The authors conducted five large-scale surveys of national populations to collect data on cognitive ability, privacy attitudes, data disclosure behaviors, and demographic variables and used binary logistic regression to analyze the relationship between these factors and susceptibility to phishing attacks. The results of the study suggest that both the willingness to share personal data and CRT scores significantly predict the probability of falling victim to phishing attempts. Additionally, age emerged as a significant predictor, albeit less influential compared to data disclosure and CRT scores. These findings are important because they suggest that phishing susceptibility is not simply a function of cognitive ability, but also of individual differences in privacy attitudes and data disclosure behaviors.

The third paper of the second session is by Van Schaik and Renaud titled "*Gauging the Unemployed's Perceptions of Online Consent Forms*," This paper reports on a study carried out to gauge unemployed users' opinions of online consent forms. After a literature review, the authors used Q-methodology to gauge agreement a number of statements related to consent forms. The authors report that unemployed people care about their data but feel pressured to consent to giving their data away when confronted with these kinds of forms. They conclude that a redesign of consent forms is required, because, in their current state, online users -- especially the unemployed -- are not granting truly informed consent.

The third session of their year's minitrack focuses on **Security Practice & Messaging**. It includes three papers that promise to incite reflection and discussion on a number of important research topics and outcomes.

The first paper of the third session is by Zhan, Durcikova and Galletta, titled "*The Paradox of Choice: Digital Akrasia in the Deployment of Two-Factor Authentication.*" This mixed-methods study examines digital akrasia, which is acting against one's better judgment because of lack of willpower. The context of the study is the voluntary adoption of multi-factor authentication (MFA). Using a mixed-method study, the authors identify factors that can mitigate digital akrasia, such as improved overall security, account verification and identify confirmation, enhanced peace of mind, and others. The others also describe factors that can increase digital akrasia, including inconvenience, time consumption, reliance on additional devices, security concerns, and so forth. The study makes a strong case that digital akrasia is a useful construct to explain security behaviors.

The second paper of the third session is by Frank, Wacker and Ranft, titled "*Same or Not the Same? Comparison Between Employees Prone to Overplacement, Overestimation and Overprecision in Information Security*." Overconfidence is a cognitive bias that can have a negative impact on information security in enterprises. This paper examines the three manifestations of overconfidence (overestimation, overprecision, and overplacement) and identifies commonalities between risk groups. The authors conducted a cluster analysis on a large-scale survey of 3,581 employees of a pharmaceutical company. They found that there were four distinct clusters of employees: "Loyal old-timers," "Young negligent," "High-income leaders," and "Committed part-timers." The authors found that the four clusters shared some commonalities, such as a lack of awareness of their own limitations and a tendency to take risks. The authors conclude that their findings can help raise awareness and understanding of overconfidence in information security, and can help design appropriate interventions.

The third paper of the third session is by Kim, Ko and Paul and is titled "*The Application of Rhetorical Theory in Designing Effective Information Security Messages for Different Leadership Styles*." This study investigates the effectiveness of fear appeal messages in changing individuals' attitudes toward security policies. The study found that fear appeal messages that appeal to pathos (emotional responses) and ethos (credibility belief) are more effective in changing individuals' attitudes toward security policies under transactional leadership. On the other hand, fear appeal messages that appeal to logos (logical judgment) are more effective in changing individuals' attitudes toward security policies under transformational leadership. This study's findings have important implications for the design of information security messages. Organizations should consider the leadership style of their employees when designing fear appeal messages. By tailoring the messaging style to the leadership style, organizations can increase the effectiveness of their messages and improve security compliance.