

Turquoise Hearte, PhD Candidate

The University of Texas at San Antonio
Department of Information Systems & Cyber Security
One UTSA Circle, San Antonio, Texas 78249
Phone: 210-980-0305(c)
Email: turquoise.hearte@utsa.edu

Research Statement

Current insider threat research focuses heavily on the malicious insider—those high-profile cases where trusted employees sabotage, steal, or remove sensitive data from their organization. Although this area of research is vital to knowledge advancement and national security, the same can and should be said for non-malicious insider threats. While it is not possible to predict specific personal circumstances that might lead an employee to unintentionally engage in risky behaviors, such as clicking on a phishing link, it is possible to identify enduring patterns of non-malicious behaviors that persist as technology evolves. My research focuses on understanding patterns of non-malicious insider threats within organizations, particularly through the lens of evolving technology adoption. In my doctoral work at the University of Texas at San Antonio, I have explored how non-malicious insider behaviors—actions that are unintentional (or intentional without malicious intent)—evolve in relation to new technological implementations, such as cloud computing and artificial intelligence.

My dissertation specifically investigates how the adoption of certain technologies impacts patterns of insider behavior, employing theories of issue evolution and actor-network theory (ANT) to understand the dynamic interplay between human and non-human actors. The goal is to uncover consistent behavioral patterns that organizations can proactively address, moving beyond reactive measures traditionally seen in organizational cybersecurity strategies.

I have had the opportunity to present my research at the SBS Insider Threat Summit in Washington D.C. with great success. Through the feedback and collaboration, I plan to continue building upon this foundation. My research trajectory will extend in several key directions:

- Future research will explore additional emerging technologies, such as artificial intelligence, cloud services, and the Internet of Things, to assess their distinct influence on non-malicious insider behaviors.
- Leveraging longitudinal studies and advanced data analytics, I plan to develop predictive models capable of identifying early indicators of non-malicious insider threats. Drawing on methodologies from my previous works, I aim to incorporate machine learning techniques that proactively identify behavioral risks associated with policy misunderstandings and compliance deviations within organizations.
- Recognizing the critical role of policy frameworks and organizational culture, my research will further examine how these factors mediate insider behavior. Specifically, I will investigate which policy designs and cultural interventions most

effectively minimize unintended, or intentional but non-malicious misuse of technology. This direction extends from my theoretical application of issue evolution and actor-network theory, integrating practical insights into policy-driven security behaviors.

The aim of this research stream is to develop actionable frameworks that organizations can adopt to proactively manage non-malicious insider threats. This involves creating evidence-based guidelines, training modules, and awareness programs tailored to specific behavioral patterns identified through my research. The ultimate objective is to equip organizations with tools to effectively anticipate and mitigate insider threats associated with new technologies.

Additionally, my research on FairPrivacy, a robust, multilingual Q&A system was presented at the Biz AI 2025 Conference as a non-procedural poster presentation to gain initial feedback and insights on the work. After sharing initial work, my co-authors and I expanded on this research, resulting in a paper that was submitted and accepted to AMCIS 2025. The paper addresses critical transparency and trust issues within the IoT consumer market. FairPrivacy was designed to bridge the comprehension gap caused by complex privacy policies, helping users understand privacy risks and device-specific vulnerabilities clearly. This research contributed important insights into how technological solutions can mitigate unintentional non-compliance and privacy threats by enhancing user comprehension and informed decision-making.

Prior to entering the PhD program, my technical area of specialty was digital forensics and Security Operations Centers (SOC) analyst work. Through that experience, I was able to collaborate and make significant contributions to work done on Virtual Reality (VR) for enhancing cybersecurity situational awareness in SOCs. This research demonstrated how immersive technologies could enhance the perception and responsiveness of novice cybersecurity operators. Published in *Computers & Security*, this study found that VR environments significantly improve users' cyber situational awareness compared to traditional methods, underscoring the potential of advanced technologies in mitigating unintentional security oversights.

Having engaged in interdisciplinary collaborations, such as my VR research in SOC environments and my exploration of consumer transparency in IoT, my future research will emphasize interdisciplinary collaborations to ensure practical relevance and applicability. These collaborations will bridge theoretical frameworks with empirical insights from cybersecurity, human-computer interaction, and organizational management domains. While both research projects pivot slightly away from the insider threat lens, it plays a critical role in my extended research interests and expertise in IoT device vulnerability analysis, SOC analysis, digital forensics, and privacy.

Through my role as lecturer, PhD student, and industry professional, I have gained unique expertise bridging theoretical knowledge and practical cybersecurity applications. My future research efforts will continue leveraging this interdisciplinary approach, significantly contributing to academic scholarship while addressing pressing organizational cybersecurity challenges as a contributing member of research