AMCIS 2019 Track: Information Security and Privacy
Mini-track: Security Breaches, Forensics, and Incident Management

Dear Colleagues,

Greetings!

We invite you to submit to the "Security Breaches, Forensics, and Incident Management" mini-track under the "Information Security and Privacy" track for AMCIS 2019 given your research related to Digital Crimes, Forensics, and Post-Incident Management. If after looking over the track and mini-track descriptions, you have questions please contact us. Thank you for reading over the call for papers and we look forward to your potential submission.

Track Description
Cybersecurity remains a key challenge for organizations despite massive investments over the last two decades. While technological advancements have been made to improve cybersecurity, human vulnerabilities have become the weakest link in security. High profile events such as defections, espionage, and massive data breaches have led the public to question their own expectations of privacy. While there is an abundance of practices and techniques for employing cybersecurity, many hard problems remain unanswered.

The purpose of this track is to provide a forum for theoretical developments, empirical research findings, case studies, methodologies, artifacts, and other high-quality manuscripts. Sponsored by SIGSEC, we seek to address important questions arising from emerging developments in information security, such as: security analytics, financial crimes, security analytics, and digital forensics? How do system defenders share information to mitigate vulnerabilities and exploits? Does pervasive data collection deter privacy-conscious individuals? Do regulations and policies influence employee security behaviors and organizational security postures?

Mini-track description
Cyber criminals increasingly target organizations to steal data and to sabotage business operations. Therefore, it is important that we constantly improve our understanding of how organizations may better detect, respond, and learn from incidents and security breaches. New knowledge will help organizational leaders minimize the adverse impacts of security breaches on operations, victims (internal and external), systems, and market performance. New knowledge may also help shield an organization from potential legal ramifications by demonstrating due diligence. In this mini-track, we explore these issues via both technical and managerial perspectives. For technologies and processes, we focus on digital forensics that are critical to effective incident and security breach responses. For management strategies, we focus on risk communication, incident response procedures, trust repair, and management of victim responses.

Modern organizations are subject to increased multi-faceted threats from security breaches. Victim organizations often suffer losses in internal operations,market performance, consumer trust, as well as legal consequences. To respond to a security incident (e.g., data breaches), organizations draw on digital forensics processes and techniques to determine cause, prosecute

offenders, and provide insight into the attack vectors deployed. Meanwhile, organizational leaders adopt management strategies to alleviate the adverse impacts of an attack on employees/customers and the society at large. Efforts are also necessary to ensure compliance with laws and regulations (e.g., GDPR). This mini-track seeks studies exploring how technical and managerial controls, policies, procedures, and options can strengthen an organization's security posture and minimize the likely impacts of security incidents. Examples topics include (but are not limited to):

- The impact of digital forensics approaches, techniques, and/or tools on an organization's defense posture and residual risk
- Digital forensic case studies
- Forensic data analytics and organizational performance
- Security policies, investment, and educational programs
- Economic impacts of security incidents on an organization
- Affective and behavioral responses of individual victims
- Trust repair strategies on victims
- Organizational response tactics on incident detection, reporting, and victim notification
- Detection of management misbehavior (e.g., insider trading) related to security breaches
- Advances in network forensics to include AI-guided IDPSs
- SIEM systems as a means to better monitor overall organizational security postures

Completed Research and ERFs submissions are due by March 1st, 2019 at 10:00 am PST.

Mini-track Chairs
Mohammadreza Mousavizadeh, m.mousavizadeh@wmich.edu
Alan Rea, alan.rea@wmich.edu

Best regards,