

2018 Americas Conference on Information Systems (AMCIS), New Orleans, LA.

Track: Information Security and Privacy

Mini-track: Digital Crimes, Forensics, and Post-Incident Management

Dear Colleagues,

We are inviting submissions to the mini track titled “Digital Crimes, Forensics, and Post-Incident Management” under the “Information Security and Privacy” track in AMCIS 2018. As you have done related research, it would be really great to have your paper included in our mini-track. Quantitative, qualitative, and design science research are all welcome. Please find the corresponding descriptions below.

Track Description

Cyber Security remains a key challenge for organizations despite massive investments over the last two decades. While technological advancements have been made to improve cyber defense, 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 cyber security, 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

Many organizations experience security breaches (e.g., data breaches) and each incident affects a victim organization with respect to its brand image and customer loyalty. To respond to a security incident, organizations draw on digital forensics techniques to determine cause, prosecute offenders, and provide insight into the attack vectors deployed. Meanwhile, organization leaders adopt management strategies to alleviate the adverse impacts of an attack on affected employees or customers. This mini-track seeks studies exploring how technical and managerial options can strengthen an organization’s security posture and minimize the likely impacts of security incidents. Examples topics include: (a) the impact of digital forensics approaches, techniques, and/or tools on an organization’s defense posture and residual risk, (b) digital forensic case studies, (c) forensic data analytics and organizational performance, (d) security policies, investment, and educational programs, (e) economic impacts of security incidents on an organization, (f) affective and behavioural responses of individual victims such as employees or customers, (g) risk communication and compensation strategies on affected victims, and (h) other topics related to organizational digital crimes and responses.

Completed Research and ERFs submissions are due by **February 28th 2018**.

Mini-Track Chairs

Mohammadreza Mousavizadeh, Western Michigan University, m.mousavizadeh@wmich.edu

Rui Chen, Iowa State University, ruichen@iastate.edu