Organizational Cybersecurity: Advanced Cyber Defense, Cyber Analytics, and Security Minitrack Overview

Miloslava Plachkinova
Kennesaw State University
mplachki@kennesaw.edu

Stuart Steiner
Eastern Washington University
ssteiner@ewu.edu

Morgan Shepherd
University of Colorado at Colorado Springs
mshepher@uccs.edu

Daniel Conte de Leon
University of Idaho
dcontedeleon@uidaho.edu

Abstract

Cybersecurity touches all aspects of organizational management, with organizational systems, networks and critical infrastructures increasingly targeted by determined malicious actors with advanced skills and resources. Such attacks have the potential for major disruption of our society including damage to assets, people, and the environment. Organizations, of all sizes and at all levels, are faced with the challenge of continuously, effectively, and efficiently protecting their systems while enabling and ensuring their mission. Organizational cybersecurity aims to advance knowledge on the theory and practice of cybersecurity management.

1. Introduction

Cybersecurity touches all aspects of organizational management, with organizational systems, networks and critical infrastructures increasingly targeted by determined malicious actors with advanced skills and resources. The goal of this minitrack is to expand research on the behaviors and practices of successful management of cybersecurity. The accepted manuscripts cover topics such as novel research or industry programs and experiences in the continuous, efficient, and effective design, engineering, implementation, operation, and management of cyber defense, cyber analytics, and security operations systems and processes within the enterprise. This includes not only the technical aspects, but also ethical and legal obligations, governance, risk, and compliance (GRC), system audits, and strategic initiatives. The minitrack also features papers from human, technical, and process perspectives on organizational cybersecurity. The following studies present a much-

needed analysis of the current issues in the field of organizational cybersecurity and provide directions for future research contributions.

This is the first year that this minitrack has been promoted at the Hawaii International Conference on System Sciences (HICSS) and submissions were from both research and industry professionals worldwide.

This year we received fifteen submissions, of which only five were accepted for publication. The 33.33% acceptance rate indicates the rigor of the conference and the quality of the published manuscripts. Each submission went through a rigorous peer-review process involving several reviewers, in addition to a follow-up round with the authors. The submissions which were accepted for publication are “My Security: An Interactive Search Engine for Cybersecurity”, “Towards Trusted Data Processing for Information and Intelligence Systems”, “Too Busy to Monitor? Board Busyness and the Occurrence of Reported Information Security Incidents”, “Organizational Aspects of Cyber Security in Family Firms: An Empirical Study of German Companies”, and “Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting”. Following are the abstracts of each paper.

2. My Security: An Interactive Search Engine for Cybersecurity

Nan Sun, Jun Zhang, Shang Gao, Leo Yu Zhang, Seyit Camtepe, and Yang Xiang demonstrate an interactive search engine that can assist cybersecurity professionals.

Large volumes of Cybersecurity-related data is generated every day from various sources at high speed to adapt to the fast-evolving landscape of cybersecurity. It drives the emergence of challenges

such as the efficient gathering of in-demand information from unstructured and heterogeneous data sources. After collecting sufficient data, it is hard for users to understand the message hidden behind the data without adequate security domain knowledge. To help address this problem, in this paper, we present My Security, an innovative search engine for gathering, managing, and understanding cybersecurity-related data. My Security is based on a novel indexing approach that stores both the information of data sources (e.g., publication date, authorship) and the pragmatics messages, including security category (e.g., ransomware, data breach) and corresponding security components (e.g., time of the event, impacted systems). With the established index, users can retrieve cybersecurity information through comprehensive approaches. Fetched results are provided with interpretations leveraged from pragmatics indexing. Additional data mining and visualization techniques enhance the interactivity of My Security by presenting the retrieved results in a clear and comprehensible manner with cybersecurity expertise. It is demonstrated that My Security is efficient at satisfying users' requirements for searching security data and helping people gain better insights into cybersecurity.

3. Towards Trusted Data Processing for Information and Intelligence Systems

Yong Wang, Kaushik Nagarajan Muthusamy Ragothaman, and Bijay Shakya discuss security implications of trusted data processing in the context of NIST's cybersecurity framework.

Data is a valued asset and its security is essential for any enterprise and organization. This paper introduces Trusted Data Processing (TDP) and addresses three fundamental questions in TDP: 1) what are the essential requirements to achieve TDP? 2) what security mechanisms and safeguards are available to ensure TDP? 3) how to integrate TDP to practice? Based on the attacks targeting at data assets and their consequences, the requirements to achieve TDP, including data security, data privacy, accountability, transparency, distributed computing, and trusted elements, are identified. Available security mechanisms and safeguards to ensure TDP are discussed. This paper also summarizes the challenges to achieve TDP and provides a practical guidance to achieve TDP through the integration with NIST Cybersecurity Framework.

4. Too Busy to Monitor? Board Busyness and the Occurrence of Reported Information Security Incidents

Carol Hsu and Tawei Wang investigated how board busyness can be associated with reported information security breaches.

This paper investigates the association between board busyness (i.e., directors with multiple positions) and the occurrence of reported information security incidents. Building on prior studies of board busyness, this paper argues that directors holding multiple board seats may fail to commit the time and effort necessary to ensure the appropriate information security strategy or investment plans are in place. Our results demonstrate that board busyness is positively associated with reported information security incidents. This effect is larger when independent directors are busy, thus suggesting the importance of the governance role played by independent directors in managing information security risks. The board of directors' role has been emphasized in anecdotal evidence and IT governance frameworks, but our study empirically demonstrates the board's relevance in information security strategy and management.

5. Organizational Aspects of Cyber Security in Family Firms: An Empirical Study of German Companies

Patrick Ulrich and Alice Timmermann present an empirical study investigating how cybersecurity is achieved in family firms in Germany.

In the context of increasing digitization and networking, the importance of cyber security is as well growing for family businesses and moving onto the management agenda as a cross-divisional, group-wide challenge. A study of 184 German companies shows that although family businesses identify cyber security as a relevant field of action, they do not sufficiently address the organizational framework and procedural implementation. This paper is dedicated to the examination of this phenomenon. Potential causes of this phenomenon will be discussed. Building on that, recommendations for action are given.

6. Perceptions of Information Systems Security Compliance: An Empirical Study in Higher Education Setting

Lei Li, Yide Shen, and Meng Han explore the perceptions of information systems security compliance in the context of higher education.

Ensuring information systems security policy compliance is an integral part of the security program of any organization. This paper investigated the perceptions of different stakeholder groups towards

information security policy compliance constructs of Unified Model of Information Security Compliance (UMISPC) in a higher education environment. The research findings showed that faculty/staff generally have higher tendency towards security policy compliance compared to students in a higher education institution. In addition, students with security knowledge are more inclined to have security policy compliance activities. Our finding not only added to the knowledge base of information systems security compliance research, but also offers practical implications.

7. Contributions and Conclusion

The Organizational Cybersecurity: Advanced Cyber Defense, Cyber Analytics, and Security minitrack at HICSS-54 focuses on research that attempts to address concerns related to cybersecurity issues in organizational settings. The growing reliance

on technology and its utilization by organizations of various sizes emphasize the need to further study this phenomenon.

The papers presented in this minitrack offer a unique and novel perspective on some of these concerns. Given the relatively new face of this research area, it is important to continue involving both practitioners and researchers with interdisciplinary backgrounds so that potential solutions can continue to be deployed in organizational settings. The studies undertaken by researchers and practitioners at various institutions should motivate our colleagues to continue working on these topics. We hope to continue providing the community with an outlet at HICSS to share their work and propose novel solutions to assist organizations with various cybersecurity issues they face.