Call for Papers
Information Systems Frontiers Special Issue on:
Behavioral issues in Cybersecurity & Privacy in the Era of Data Explosion

Overview:
Astronomical amounts of data are being generated, captured, copied and stored every day (Overberg and Hand 2021). Statista estimates that by 2025, the world will have produced over 180 Zetabytes of data (Statista 2023). Businesses are increasingly relying on those data to gain insights into their employees (Ng et al. 2021), contractors/suppliers (Wall et al. 2022), and customers' behaviors and preferences (Wang et al. 2022). While using data in creative ways is a powerful tool for driving business growth, it also presents significant risks (Wynn 2023). The larger the volume of data, the larger the security risk to the organization (Yi et al. 2023). Further, the sudden popularity of using AI and other emerging techniques for data processing and analysis have strong implications for cybersecurity in organizations.

Humans have been the "weakest link" in the cybersecurity chain (Bulgurcu et al. 2010) and still continue to be of utmost significance today (Hughes-Lartey et al. 2021). In a recent report (Verizon 2023), Verizon reports that 74% of all data breaches involve some degree of human element. Given the vast volume of data, the negative outcomes of data breaches are exponentially worse. Governments, organizations, employees, and consumers all play a role in the mitigation of cybersecurity risk through the behaviors they encourage or enact to protect the security and privacy of data (Gupta et al. 2018; Krishna et al. 2022). Examining human behavioral issues focusing on cybersecurity in this intricate data-driven landscape will become more and more crucial in this context.

While there have been special issues in the past in ***Information Systems Frontiers (ISF)***, focusing on cybersecurity from the lenses of secure knowledge management (Hota et al. 2015; Sahay et al. 2021; Samtani et al. 2023), data leakage (Huth et al. 2013), ethics and privacy (Acquisti et al. 2019), foundations (Xu et al. 2021) and economic aspects (Gordon and Loeb 2006), this special issue specifically focuses on emerging behavioral issues in cybersecurity arising from the present data explosion. This **special issue** aims to provide insights into both present and future approaches to cybersecurity by developing theoretical and practical understandings of behavioral issues in cybersecurity relevant to the industry today. We welcome conceptual, theoretical, empirical, experimental, methodological, and practice-based papers that enrich our understanding of cybersecurity in this present era of data explosion.

Topics of interest include, but are not limited to:
- Human-centric and behavioral issues in cybersecurity (e.g., insider threat)
- Cultural issues in security and privacy
- Socio-technical analysis of security and privacy
- Cybercrime, cyber threat intelligence, detection, and mitigation

- Cybersecurity risk analysis, threat assessment and incident response
- Societal and ethical issues in cybercrime
- Cybersecurity education, pedagogy, and skill development
- Future directions in security and privacy

Submission:
This special issue will consist of papers from two sources: (1) the best submissions from an open call for papers, and (2) invited submissions that are substantial revisions of selected papers accepted at the **2023 Pre-ICIS Workshop on Information Security and Privacy (WISP)**. The submitted manuscript is required to have a more than 40% new and original technical or scientific content, distinct from the conference paper. Authors will be required to submit a letter detailing the differences between the conference paper and the version submitted to this special issue of *Information Systems Frontiers (ISF)*.

All submissions will go through a comprehensive peer review process and each submission will be evaluated by at least two independent reviewers. Submissions must be written in proof-read English and submitted in PDF format via the editorial manager of the journal: https://www.editorialmanager.com/isfi/default.aspx.

To ensure that the manuscripts are correctly submitted to this special issue, authors must select "Emerging Tech" as the "Article Type." Authors should aim at papers of approximately 25 to 30 pages (in the submission format, 11 Font, 1.5 line spacing, including abstract, figures, tables, references and appendix), following the submission guidelines from the journal: https://www.springer.com/journal/10796/submission-guidelines

Important Dates:
Submission deadline: 1st March 2024
Notification of first round reviews: 1st July 2024
Revised manuscript due: 1st October 2024
Notification of second round reviews: 15th November 2024
Final version due: 1st Jan 2025
Tentative publication date: 15th March 2025

Guest Editors:
Sumantra Sarkar (ssarkar@binghamton.edu), Binghamton University, Binghamton, NY
Philip Menard (philip.menard@utsa.edu), UTSA, San Antonio, TX
Scott Boss (sboss@bentley.edu), Bentley University, Waltham, MA

Guest Advisory Editor:
Anthony Vance (anthony@vance.name), Virginia Tech, Blacksburg, VA

Sumantra Sarkar is an associate professor in Management Information Systems at the School of Management, State University of New York (SUNY), Binghamton. He received his Ph.D. from the Computer Information Systems department at Georgia State University. He has a MS in Computer Information Systems (Health Informatics), an MBA in Operations Research, and holds

PMP and CISA certifications. His research interests include IT security, health information technology, organizational processes, agile development, and IT governance. His work has appeared in premier IS journals like *ISR, JMIS, EJIS, ISJ, IJIM, CAIS, JBR* and *IEEE IT Professional*. He actively volunteers for the information systems community reviewing for conferences/journals and is presently a SE for *The Data Base for Advances in Information Systems*.

Philip Menard is an associate professor of Information Systems and Cyber Security at the University of Texas at San Antonio. He received his PhD from the Department of Management and Information Systems at Mississippi State University. He is interested in the impacts of security measures on organizational end users, security education training and awareness (SETA) programs, privacy implications of machine learning implementations, and socio-technical impacts of fake news propagation and consumption. He has published at *JMIS*, *JAIS*, *EJIS*, *ISJ*, *Computers & Security*, *Information & Management*, *Information Systems Frontiers*, and *JCIS*. He has presented his work at several conferences and workshops and has served as a reviewer for several IS journals and conferences.

Scott Boss is an associate professor at the Department of Accountancy, Bentley University. He holds a Ph.D. in Information Systems from the University of Pittsburgh. His research concentrates on information security, controls, cybercrime, and fraud. His work has been published in *MISQ, EJIS*, Group and Organization Management, International Journal of Accounting Information Systems, and Business Process Management Journal. He is one of the founding members of the IFIP WG8.11/ WG11.13 Dewald Rood International Workshop on IS Security Research. Prior to his work in academia, Scott worked as a systems auditor and cybersecurity consultant at two different public accounting firms. Scott teaches classes on advanced accounting information systems, cybersecurity, and fraud and forensics at Bentley University.

Anthony Vance is the Lenz Professor and Commonwealth Cyber Initiative Fellow in the department of Business Information Technology of the Pamplin College of Business at Virginia Tech. He earned Ph.D. degrees in Information Systems from Georgia State University, USA; the University of Paris—Dauphine, France; and the University of Oulu, Finland. Previous to his PhD studies, he worked as a cybersecurity consultant at Deloitte. His research focuses on how to help individuals and organizations improve their cybersecurity posture, particularly from behavioral, organizational, and neuroscience perspectives. His work is published in outlets such as *MISQ, ISR, JMIS, JAIS*, Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI), Workshop on the Economics of Information Security (WEIS), and the Symposium on Usable Privacy and Security (SOUPS). He currently is a senior editor at *MIS Quarterly*.

References:

Acquisti, A., Dinev, T., and Keil, M. 2019. "Editorial: Special Issue on Cyber Security, Privacy and Ethics of Information Systems," *Information Systems Frontiers* (21:6), pp. 1203-1205.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. ," *MIS Quarterly* (34:3), pp. 523-548.

Gordon, L. A., and Loeb, M. P. 2006. "Economic Aspects of Information Security: An Emerging Field of Research," *Information Systems Frontiers* (8:5), pp. 335-337.

Gupta, A., Deokar, A., Iyer, L., Sharda, R., and Schrader, D. 2018. "Big Data & Analytics for Societal Impact: Recent Research and Trends," *Information Systems Frontiers* (20), pp. 185–194.

Hota, C., Upadhyaya, S., and Al-Karaki, J. N. 2015. "Advances in Secure Knowledge Management in the Big Data Era," *Information Systems Frontiers* (17:5), pp. 983-986.
Hughes-Lartey, K., Li, M., Botchey, F. E., and Qin, Z. 2021. "Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things," *Heliyon* (7:3).
Huth, C. L., Chadwick, D. W., Claycomb, W. R., and You, I. 2013. "Guest Editorial: A Brief Overview of Data Leakage and Insider Threats," *Information Systems Frontiers* (15:1), pp. 1-4.
Krishna, B., Krishnan, S., and Sebastian, M. 2022. "Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective," *Information Systems Frontiers*), pp., 1–29.
Ng, K. C., Zhang, X., Thong, J. Y. L., and Tam, K. Y. 2021. "Protecting against Threats to Information Security: An Attitudinal Ambivalence Perspective," *Journal of Management Information Systems* (38:3), pp. 732-764.
Overberg, P., and Hand, K. 2021. "How to Understand the Data Explosion." Retrieved Sep 2, 2023, from https://www.wsj.com/articles/how-to-understand-the-data-explosion-11638979214
Sahay, S. K., Goel, N., Jadliwala, M., and Upadhyaya, S. 2021. "Advances in Secure Knowledge Management in the Artificial Intelligence Era," *Information Systems Frontiers* (23:4), pp. 807-810.
Samtani, S., Zhao, Z., and Krishnan, R. 2023. "Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence," *Information Systems Frontiers* (25:2), pp. 425-429.
Statista. 2023. "Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2020, with Forecasts from 2021 to 2025." Retrieved Sep 2, 2023, from https://www.statista.com/statistics/871513/worldwide-data-created/
Verizon, E. 2023. "2023 Data Breach Investigations Report." Retrieved Sep 2, 2023, from https://www.verizon.com/business/resources/reports/dbir/
Wall, J. D., Palvia, P., and D'Arcy, J. 2022. "Theorizing the Behavioral Effects of Control Complementarity in Security Control Portfolios," *Information Systems Frontiers* (24:2), pp. 637-658.
Wang, Y., Currim, F., and Ram, S. 2022. "Deep Learning of Spatiotemporal Patterns for Urban Mobility Prediction Using Big Data," *Information Systems Research* (33:2), pp. 579-598.
Wynn, R. 2023. "Big Data, Big Risks: How Startups Can Safeguard Their Customers' Information." Retrieved Sep 2, 2023, from https://www.forbes.com/sites/forbestechcouncil/2023/04/13/big-data-big-risks-how-startups-can-safeguard-their-customers-information/?sh=3c927936cdbf
Xu, S., Yung, M., and Wang, J. 2021. "Seeking Foundations for the Science of Cyber Security," *Information Systems Frontiers* (23:2), pp. 263-267.
Yi, Y., Yu, Q., Yangyang, F., and Zhongju, Z. 2023. "Unlocking the Power of Voice for Financial Risk Prediction: A Theory-Driven Deep Learning Design Approach," *MIS Quarterly* (47:1), pp. 63-96.