Organizational Cybersecurity Journal editorial introduction

Editorial

Technical cybersecurity dominates discussion and investment even though there is a realization to approach cybersecurity problems from organizational cybersecurity or information security management perspectives. The technical focus is further reflected in the predominance of technical education programs and even "Capture-the-flag" competitions. Yet, calls to focus on the management aspects of protecting information assets or considering the business risks can be traced back over half a century. In an article entitled "Danger Ahead! Safeguard Your Computer," the author raises ". . . serious questions about security for the management to consider: Could the company continue to transact its business if its computer center and everything in it were suddenly destroyed? Has the company properly protected its programs, files, and equipment against sabotage?" (Allen, 1968, p. 97). The author further notes (p. 101):

> Although perfect security systems, as always, are beyond reach, a company can implement a very satisfactory one at reasonable cost. What is needed most right now is management's awareness of the problem, an appreciation of the hazards involved and a determination to prevent severe misfortunes.

Shortly after that warning, Sorensen (1972) opened an article with words that continue to resonate and are reflected in everyday news stories (p. 379):

> Suddenly, everyone's concerned about computer security . . . New Companies have been formed specializing in products that provide better security in a computer department; and seminars are being offered around the country dealing with control and security of computer installations. Management is concerned. It has realized that its computer department, the heart of its day-to-day vital information and control system, has unique vulnerability to theft, disruption and destruction.

Our chosen area of cybersecurity management is still considered to be a nascent field and needs nurturing. Cybersecurity impacts not only the technical side of an organization but also brand image, ethical and legal obligations, continuing operations, customer relations, internal processes, risk management, system audits, strategic initiatives and almost every dimension of sustaining and growing a successful organization. We collectively have a shared responsibility to get actively involved and mold it towards a mature management discipline.

Of the many journals that publish cyber and computer security research, most focus on technology, systems, crime and data protection. Those that consider organizational issues cover a very broad scope and do not zero in on the aspects that impact organizations. *Organizational Cybersecurity Journal: Practice, Process, and People (OCJ)* seeks to publish advances in scientific knowledge directly related to cybersecurity management. We target research relating to the behaviors and practices that influence the successful management of cybersecurity. The journal welcomes papers from human, technical and process perspectives on the topic. We endeavor to establish this journal as a prominent journal in the emerging discipline of cybersecurity.

Organizational Cybersecurity
Journal: Practice, Process and
People
Vol. 1 No. 1, 2021
pp. 1-4
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-09-2021-017

Why cybersecurity (not information systems security)?

We echo the sentiments of Curtin (2017): "Call it cybersecurity, information security, data security, or information assurance; the world has a problem with it," (p. 1). We can add computer security, information technology security and information system security to the above statement, all of which have unique nuances. The world (government, industry and media) seems to be coalescing towards using a single term, cybersecurity, in place of various terms denoting different facets of securing information and critical infrastructure. The Joint Task Force on Cybersecurity Education (JTF) – representing collaboration between the major international computing societies of the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC) and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) – adopted a similar approach. We sheepishly decide to follow the guidance of the JTF in the following.

Definition

The JTF defines cybersecurity as "A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (JTF, 2017, p. 16). The people, information and processes are the purview of cybersecurity management or organizational cybersecurity.

Challenges

The cybersecurity landscape is complex and uncertain. The creation and use of information attain value within the context of organizations. Securing such information gets complicated due to organizational members (insiders), users (customers), regulations and cyber-miscreants. The users want access to information anytime and anywhere, and cybersecurity professionals need to design security for such complex information systems. Additionally, there are increased regulations to follow, often written by non-cybersecurity experts. Then, there is the nuisance of cyber-miscreants that led to the emergence of an underground cybercrime economy. The field attracted organized crime and hacking groups (along with hacktivists), resulting in the increased industrialization of cybercrime estimated to be in the trillions of dollars.

Focus

The goal of organizational cybersecurity should be to efficiently protect critical information assets (along with infrastructure) while attaining organizational objectives. Since the early days of addressing this problem, there has been an emphasis on securing only critical data or information. However, over the past decade, both practitioners and researchers have dropped this sole emphasis. We should not be surprised to find subsequent solutions providing mixed results in protecting critical information and impact on business (especially in terms of cost-effectiveness). We wish to draw the focus back to the protection of critical information and infrastructure while considering the constraints of organizations. Such endeavors will help us acknowledge the limited resources available to an organization or society (tipping our hat to economists) and pay attention to the intricate complexities of an organizational environment with social, political, psychological and economic forces at play.

Approach

OCJ encourages rigorous research focused on, but not limited to, cybersecurity governance, managing information security, behavioral and cognitive cybersecurity, compliance and audit, business process assurance, digital privacy and ethics and secure use of emergent technologies. The journal will publish quarterly issues predominantly focusing on research and conceptual papers. Conceptual papers will develop hypotheses and be discursive, covering philosophical discussions and comparative studies of other works and thinking. The editorial team's approach is developmental, with constructive feedback, editorial transparency and reasonable turnaround from submission to publishing. We are paradigm and method agnostic believing in the value of diverse views and pluralism in scientific endeavor. Our editors are committed to supporting authors in finding the best version of their paper with an explicit contribution in the context of organizational cybersecurity.

Societal benefit

The Editorial Board firmly believes in disseminating the research results to a wider public for societal benefit. OCJ is published under a Platinum Open Access arrangement, in that there is no charge to the author, and all articles are made freely available in their entirety to the public. We sincerely thank the State of Colorado and the University of Colorado Colorado Springs College of Business for providing funds and necessary support. OCJ follows the guidelines provided by the Committee on Publication Ethics (COPE) to ensure the content is ethically sound.

First issue

The papers appearing in the inaugural first issue focus on behavioral and cognitive cybersecurity, with one paper addressing the organizational concerns of small- and medium-sized enterprises (SMEs). These papers represent a balance between American and European perspectives. Botong Xue, Feng Xu, Xin Luo and Merrill Warkentin emphasize the role of ethical leadership in influencing employees' security behavior by drawing on social learning and social exchange theories. The results indicate that ethical leadership influences employees' information security policy violation intention through information security climate rather than affective commitment. Karen Renaud and Jacques Ophoff promote understanding why SMEs do not implement cybersecurity best practice measures. The authors' developed a cyber-situational awareness model based on the theory of situational awareness. The results highlight the influence of understanding the importance of cybersecurity, followed by the availability of resources.

Molly Cooper, Yair Levy, Ling Wang and Laurie Dringus introduce the concept of audiovisual alerts and warnings as a way to reduce phishing susceptibility. The authors test a prototype developed on the premise that the alerts and warnings can trigger "System 2 Thinking Mode" proposed by Daniel Kahneman. The results from a three-phased study indicate audio alerts and visual warnings potentially lower phishing susceptibility in emails. Kavya Sharma, Xinhui Zhan, Fiona Nah, Keng Siau and Maggie Cheng also explore how to reduce user susceptibility to phishing and extend the concept of digital nudging from the human-computer interaction field. The authors examine the impact of framing and priming on users' behavior in a cybersecurity setting. The study draws on prospect theory, instance-based learning theory and dual-process theory. The results establish the role of digital nudging in the form of priming to reduce users' exposure to cybersecurity risks. In doing so, they also demonstrate the primacy of instance-based learning theory in the context of cybersecurity behavior.

We sincerely hope our readers will find these research papers to be stimulating. We invite you to participate in the journal as contributing author, reviewer, or special issue editor. Feel free to contact us with suggestions or proposals.

Gurvirender Tejay and Gary Klein

References

Allen, B. (1968), “Danger ahead-safeguard your computer”, *Harvard Business Review*, Vol. 46 No. 6, pp. 97-101.

Curtin, C.M. (2017), “Protection of Data and Prevention: Advice for Chief Executive Officers, Managers, and Information Technology Staff”, *Interhack Report (5/5)*, available at http://web.interhack.com/publications/protection-prevention.pdf (accessed 29 August, 2021).

JTF (Joint Task Force on Cybersecurity Education) (2017), *Cybersecurity Curricular Guidelines*, CSEC, available at: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf (accessed 30 August 2021).

Sorensen, J.L. (1972), “Common sense in computer security”, *The CPA Journal*, Vol. 42 No. 5, p. 379.