Call for Papers

A Special Feature of the *Journal of Business and Psychology*

Security, Privacy, and Surveillance in Cyberspace: Organizational Science Concerns and Contributions

Special Issue Guest Editors:

Reeshad S. Dalal, Rebecca J. Bennett, and Clay Posey

Special Issue Editorial Board:

Bradley J. Alge, David A. Askay, Glory Emmanuel Aviña, Talya N. Bauer, Devasheesh P. Bhave, Bradley J. Brummel, Matthew A. Cronin, Peter D. Harms, David J. Howard, Allen C. Johnston, Mala Kaul, Mindy Shoss, Shashi K. Srivastava, and Donald M. Truxillo

Objective

This special issue follows a paper recently published in the *Journal of Business and Psychology* (Dalal et al., in press). The goal of the current special issue, building on the recent paper, is to catalyze micro-, meso-, and macro-organizational science research on cyber security, privacy, and surveillance. We welcome submissions that emphasize knowledge transfer from organizational science to cyber security, privacy, and/or surveillance as well as submissions that emphasize knowledge transfer in the opposite direction.

Description

The Internet has transformed the way organizations and employees function, greatly improving workflow and communication. Yet, these benefits have been accompanied by considerable and continually proliferating concerns involving cyber security, privacy, and surveillance. Large and small organizations around the world are targets of cyber attacks, leaving their operations, their employees, and their customers vulnerable. Most readers of this Call for Papers have, knowingly or unknowingly, already been victims of cyber breaches.

Yet, in spite of the urgency of this problem, organizational science research (e.g., Bauer et al., 2020; Bernstein, 2017; Bhave et al., 2020; Brady et al., in press; Dalal et al., in press; Ravid et al., 2020; Zaccaro et al., 2016) and guides to evidence-based practice (e.g., Dreibelbis et al., 2018; Tetrick et al., 2016) in, or of relevance to, the domains of cyber security, privacy, and surveillance remain in their infancy. Peer-reviewed journal articles and guides to practice and policy in these domains are, instead, mostly associated with the disciplines of computer science, information systems, information technology, and the law, among others. This is unfortunate because, although attacks on information systems tend to be highly technical in nature, cyber attacks, privacy breaches, and digital surveillance are enacted by people (e.g., “hackers,” disgruntled employees, supervisors), groups of people (e.g., criminal gangs, intelligence agencies from nation-states, organizations), or technology programmed by people (e.g., “bots”). Similarly, the targets of and defenders against cyber attacks, privacy breaches, and digital surveillance are also people (e.g., employees), groups of people (e.g., organizations, nation-states, Cyber Security Incident Response Teams), or technology programmed by people (e.g., web servers, Security Information and Event Management software). Cyber security researchers (e.g., Pfleeger & Caputo,

2012)—and, in our experience, cyber security-focused employees and their leadership in organizations—themselves recognize the potential for appreciable contributions from the social and behavioral sciences, including the organizational sciences. Additionally, existing attempts at meta-theories of privacy, let alone cyber privacy in particular, have not emanated from organizational science researchers (Bernstein, 2017; though cf. Bhave et al., 2020). The time has therefore come for organizational scientists to contribute to, as well as to learn from, research in cyber security, privacy, and surveillance.

We welcome submissions on topics including, but not limited to, the following:

- *The increasing cyber security, privacy, and surveillance components of "regular" (non cyber security-focused) jobs.* For example, what are the security, privacy, and/or surveillance implications when employees are hired and trained online—and how can these implications be connected to existing organizational science theories? Which individual differences variables (personality, cultural values, knowledge, skills, abilities, demographic characteristics, etc.) contribute to susceptibility versus resilience to cyber attacks (e.g., phishing attacks) and/or influence perceptions of privacy violation? Does cyber security training contribute to safer or simply more risk-averse behavior (Dalal et al., in press; Proctor & Chen, 2015)?
- *The "criterion problem" (Austin & Villanova, 1992) as it applies to cyber security and/or privacy*—see, for example, Posey et al. (2013) regarding "protection-motivated behaviors." In that vein, what metrics, or key performance indicators, should be used to assess the job performance of cyber-specific roles in organizations, such as individual cyber security analysts, Cyber Security Incident Response Teams, or Chief Information Security Officers? Further, how can/should we measure cyber-related job performance when success involves "non-events" that are by definition hard to observe (e.g., correct non-response to phishing attempts by end-users, thwarted privacy breaches by cyber security-focused employees)? To what extent can a proper assessment of employee cyber security performance—that is, one that avoids criterion deficiency and contamination—be conducted through "objective" methods alone (e.g., electronic performance monitoring for actual behaviors, and physiological and neuroscientific approaches for employee decisions, which result in successful "non-events"); in other words, to what extent might self- and other-reports of performance still prove necessary?
- *Insider threat and its conceptual and/or empirical connections to constructs studied by organizational researchers.* For example, to what extent should the taxonomies/typologies, theories, measures, and antecedents of insider threat differ from those associated with counterproductive or deviant work behavior (Robinson & Bennett, 1995; see, e.g., Dalal et al., in press; Dalal & Gorab, 2016), whistleblowing (Anvari et al., 2019; Culiberg & Mihelič, 2017), or other such constructs studied in organizational science? What can organizational science researchers learn from the study of insider threat?
- *Team and multiteam system functioning in a cyber security context.* For example, what are the best ways for human team members to develop trust in and team mental models with cyber-enabled technological "teammates" (e.g., machine learning algorithms or more broadly artificial intelligence)?
- *The role of social networks.* For example, what are the potential risks of social networks (and spillover across personal and workplace networks), especially risks facilitated by cyber technologies (i.e., social media), in terms of unauthorized disclosure of proprietary information? How do social

and information communication technology networks interact in determining organizational cyber security?

- *Macro (e.g., organization-level, industry-level and national/societal-level) factors influencing cyber security, privacy, and/or surveillance.* For example, how can organizations transition from "checklist compliance" cultures to cultures that actively mitigate harm to information assets (Burns et al., 2018)? What is the interplay between macro factors (e.g., industry, organizational structure, culture/climate, and policies and procedures) and micro factors (e.g., individual differences in employee risk perceptions) in predicting employee cyber security behavior?
- *Cyber security executive leadership.* For example, which competencies matter for leaders/executives in cyber security? What are the key challenges facing executive leaders in cyber security?
- *Designing meaningful and healthy cyber security work and careers.* For example, can the precision of organizational science theories aimed at predicting and minimizing burnout and turnover be improved to take account of a multitude of objective job characteristics, so that these theories can make precise predictions about specific occupations such as cyber security occupations (which are high-turnover occupations, potentially because of the repetitive, exacting, stressful, and shift-driven nature of the work)?
- *Unique aspects of diversity, discrimination, and harassment as they pertain to cyber security, privacy, and/or surveillance.* For example, to what extent are other deviant cyber behaviors (e.g. cyber bullying and ostracism) antecedents to malicious cyber security/privacy violating behaviors?
- *Implications of the changing nature, locations, and schedules of work for cyber security, privacy, and/or surveillance.* For example, what unique privacy concerns are engendered via videoconferencing when employees take work meetings from home, and what are the attitudinal and performance-based effects on employees? Similarly, what privacy implications emerge when organizations request certain changes be made to an employee's home-based work environment?
- *Implications of the convergence over time between the cyber and physical worlds (e.g., cyber-physical systems such as the Internet of Things and augmented reality) and novel cyber-related technologies for organizational science.* For example, what are the implications of blockchain and other distributed ledger technology for traditional organizational science theories of trust?
- *Research ethics, employee and organization rights and responsibilities, and so forth as they pertain to organizational science research on cyber security, privacy, and/or surveillance.* For example, to what extent do the "lenses" used to conceptualize employee privacy (e.g., privacy as a commodity vs. privacy as a right) differ across employees, across organizations, and between employees and organizations? What guidance can the organizational science methodological literature (e.g., Bliese & Lang, 2016; Rudolph et al., 2020) provide regarding how changes in employee perceptions of privacy can effectively be tracked over time and as a function of specific technological developments (e.g., the Internet, social media)?
- *Conceptual frameworks, empirical research designs, and data-analytic approaches used by other disciplines that study cyber security, privacy, and surveillance that are novel in, and should be "imported" to, organizational science—and/or vice versa.* For example, what are the similarities and differences between the research literatures on cyber surveillance and organizational research on electronic performance monitoring? In determining employee perceptions of psychological contract breach, how important are breaches in employee information privacy relative to more traditional organizational science predictors?

- *Meta-theories aimed at integrating organizational cyber security, privacy, and surveillance—and their consequences.* For example, could a risk-benefit "calculus" (Bhave et al., 2020; Wiederhold, 2014), a cybernetic control theory perspective (Vancouver, 2020), or a cognitive psychology-based information processing perspective (Proctor & Chen, 2015) parsimoniously integrate these constructs and clarify their relative importance with regard to employee cognitive-affective and behavior/performance reactions?
- *Cyber security, privacy, and surveillance concerns arising from COVID-19.* For example, what are the impacts, both negative and positive, of employee privacy concerns related to organizational COVID-19 mitigation efforts (based on potentially intrusive health-symptom online questionnaires, contact tracing via the physical and temporal proximity of employee smartphones connected to the organization's wireless network, etc.)? Importantly, how can such research be tied to existing organizational science theories?
- *Other topics discussed as future research needs* in the recent Dalal et al. (in press) paper in this journal or in the cyber-relevant portions of Bernstein (2017), Bhave et al. (2020), Ravid et al. (2020), and other review papers.

We welcome submissions focused at the individual employee, team, multiteam system, and/or organization level of analysis. We welcome submissions focused on cyber security jobs as well as submissions focused on "regular" end-users for whom cyber security (and privacy and surveillance) concerns are increasingly intertwined with regular task behavior.

We welcome cross-case syntheses (but not single case studies), grounded theory approaches, natural language processing studies, survey designs (traditional survey designs, experience sampling methods, etc.), laboratory or field experiments, policy-capturing studies, intervention studies, narrative reviews, meta-analyses, conceptual papers, computational models, and mixed qualitative and quantitative designs, among others. Submissions based on laboratory experiments or policy-capturing studies should explicitly address the external validity of stimuli, settings, and samples. Meta-analytic submissions should contribute to theory testing or development, and should include a focus on publication source discipline (e.g., organizational science vs. information security) and publication quality (e.g., as a moderator variable or through inclusion criteria) in addition to publication bias. Computational model submissions should reference existing organizational science theories, should be accompanied by adequate verbal description, and should discuss model testing/validation. Scale development submissions should include theory testing or development—that is, construct validation through the development of nomological networks—along with methodological rigor. Submissions that use participant panels (e.g., Prolific, Mechanical Turk) should adhere to best practices aimed at ensuring data quality and avoiding participant misrepresentation.

Submissions to the special issue should clearly demonstrate familiarity not just with relevant organizational science literature but also with relevant cyber security, privacy, and/or surveillance literatures. Additionally, due to the tendency to use different labels across research disciplines to refer to similar phenomena or constructs (the "jangle fallacy"), and perhaps also the tendency to use the same label to refer to different phenomena or constructs (the "jingle fallacy"), submissions should address construct uniqueness versus redundancy issues, for instance by including formal construct definitions and, if appropriate, by demonstrating the incremental validity of focal constructs beyond plausible alternatives.

If you have any questions about this special issue (e.g., about the “fit” of a potential submission), please do not hesitate to email one or more of the Guest Editors (rdalal@gmu.edu, rebecca.bennett@ucf.edu, and/or m.clay.posey@gmail.com), with email subject line “JBP Cyber Special Issue.”

Submission Details

Manuscript submissions are due by **February 15, 2022**.

Manuscripts must be prepared according to the manuscript submission guidelines for the *Journal of Business and Psychology* homepage (https://www.springer.com/journal/10869/submission-guidelines). We welcome “regular” submissions as well as manuscripts submitted under the journal’s “results-blind review” initiative (https://jbp.uncc.edu/). Manuscripts should be submitted to the journal's manuscript submission portal (https://www.editorialmanager.com/jobu). Regular submissions to this special issue should use the "Security, Privacy, and Surveillance regular submission track" author submission option in the system, whereas results-blind submissions should use the "Security, Privacy, and Surveillance results-blind submission track."

Submissions will undergo an initial editorial review by the guest editors. Those meeting criteria for further consideration will undergo masked peer-review.

References

Anvari, F., Wenzel, M., Woodyatt, L., & Haslam, S. A. (2019). The social psychology of whistleblowing: An integrated model. *Organizational Psychology Review*, *9*(1), 41-67.

Austin, J. T., & Villanova, P. (1992). The criterion problem: 1917–1992. *Journal of Applied Psychology*, *77*(6), 836-874.

Bauer, T. N., Truxillo, D. M., Jones, M. P., & Brady, G. (2020). Privacy and cybersecurity challenges, opportunities, and recommendations: Personnel selection in an era of online application systems and big data. In S. E. Woo, R. Proctor, & L. Tay (Eds.), *Big data in psychological research* (pp. 393-409). Washington DC: APA.

Bernstein, E. S. (2017). Making transparency transparent: The evolution of observation in management theory. *Academy of Management Annals*, *11*(1), 217-266.

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, *46*(1), 127-164.

Bliese, P. D., & Lang, J. W. (2016). Understanding relative and absolute change in discontinuous growth models: Coding alternatives and implications for hypothesis testing. *Organizational Research Methods*, *19*(4), 562-592.

Brady, G., Truxillo, D. M., Bauer, T. N., & Jones, M. P. (in press). Development and validation of the Privacy and Data Security Concerns Scale (PDSCS). In press at *International Journal of Selection and Assessment*.

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of insiders' awareness of organizational SETA efforts. *Decision Sciences, 49*(6), 1187–1228.

Culiberg, B., & Mihelič, K. K. (2017). The evolution of whistleblowing studies: A critical review and research agenda. *Journal of Business Ethics*, *146*(4), 787-803.

Dalal, R. S., & Gorab, A. K. (2016). Insider threat in cyber security: What the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Psychosocial dynamics of cyber security* (pp. 92–110). New York, NY: Routledge.

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (in press). Organizational science and cybersecurity: Abundant opportunities for research at the interface. In press at *Journal of Business and Psychology*. Open Access: Full-text available at https://link.springer.com/article/10.1007/s10869-021-09732-9

Dreibelbis, R. C., Martin, J., Coovert, M. D., & Dorsey, D. W. (2018). The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. *Industrial and Organizational Psychology, 11*(2), 346–365.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597-611.

Posey, C., Roberts, T., Lowry, P., Bennett, R., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189-1210.

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace. *Human Factors*, *57*(5), 721-727.

Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management*, *46*(1), 100-126.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555–572.

Rudolph, C. W., Costanza, D. P., Wright, C., & Zacher, H. (2020). Cross-temporal meta-analysis: A conceptual and empirical critique. *Journal of Business and Psychology*, *35*(6), 733-750.

Tetrick, L. E., Zaccaro, S. J., Dalal, R. S., Steinke, J. A., Repchick, K. M., Hargrove, A. K., Shore, D. B., Winslow, C. J., Chen, T. R., Green, J. P., Bolunmez, B., Tomassetti, A. J., McCausland, T. C., Fletcher, L., Sheng, Z., Schrader, S. W., Gorab, A. K., Niu, Q., & Wang, V. (2016). *Improving social maturity of cybersecurity incident response teams.* Fairfax, VA: George Mason University. Retrieved from http://calctraining2015.weebly.com/the-handbook.html

Vancouver, J. B. (2020). Perceptions of control theory in industrial-organizational psychology: Disturbances and counter-disturbances. In W. Mansell (Ed.), *The interdisciplinary handbook of perceptual control theory: Living control systems IV* (pp. 463-501). London, U.K.: Academic Press.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. In *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131-132.

Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., Steinke, J. A. (Eds.) (2016). *Psychosocial dynamics of cyber security.* New York, NY: Routledge.