12-15-2019

Burnout in cybersecurity professionals

Obi Ogbanufe

Janine Spears

Burnout in Cybersecurity Professionals

Obi Ogbanufe [1]
Spears School of Business, Oklahoma State University,
Stillwater, Oklahoma, USA

Janine Spears
Monte Ahuja College of Business, Cleveland State University,
Cleveland, Ohio, USA

ABSTRACT

The cybersecurity profession is critically understaffed. Coupled with the increase in cyber threats, cybersecurity professionals are experiencing burnout. Burnout among cybersecurity professionals can have a negative effect on an organization's ability to ward off aggressive breach attempts from cyber-adversaries. The Maslach Burnout Inventory (MBI) scale has been used to measure burnout in information systems (IS) and other professions. This study extends the MBI literature. In particular, we suggest that the cybersecurity profession has unique characteristics that warrant further investigation into how the scale relates. This research-in-progress examines burnout in the cybersecurity profession by identifying context-specific job characteristics related to the role. A conceptual model and propositions are provided, including a proposed methodology and expected results.

Keywords: Maslach burnout inventory, cybersecurity profession, cybersecurity burnout, role identity

INTRODUCTION

Researchers and practitioners agree that cybersecurity is a key issue for organizations (Kappelman et al. 2018). In a recent survey of leaders at the 2019 World Economic Forum, cybersecurity was listed as the number one concern for CEOs in the U.S (Reid 2019). With a near 0% percent unemployment rate recorded in 2016 and a forecast of almost 3.5 million

[1] Corresponding author. obi.ogbanufe@okstate.edu.edu +1 405-744-9730

positions unfilled, the cybersecurity job market has been experiencing a severe talent shortage since 2016 (Morgan 2017). In the U.S. alone, the demand for cybersecurity roles increased by 7% between 2017 and 2018 (Indeed 2019), an increase attributed to the incessant cyber-attacks on organization. As organizations grapple with addressing both the evolving cybersecurity threat landscape and the severe shortage in cybersecurity personnel, currently employed cybersecurity professionals are increasingly facing work exhaustion, burnout, and leaving the workforce. Studies have noted the prevalence of burnout in cybersecurity professions (Dykstra and Paul 2018; Hull 2017), as have practitioners (CSO 2019; Schueler 2019).

Burnout among cybersecurity professionals can have a negative effect on the organization's ability to keep up with warding off aggressive breach attempts from cyber-adversaries. Other psychological and physiological impacts from burnout could be more severe, ranging from substance abuse to depression and suicide (Corman 2019). Thus, the problem of cybersecurity burnout has received increased attention in industry. As evidence of its importance, Christina Maslach was invited to give the keynote in 2019 at one of the industry's largest conferences, the RSA Conference, to discuss burnout within the cybersecurity profession[2].

The nature of the cybersecurity professional's job is complex, demanding, and never ending. Cybersecurity professionals are the experts that protect organizational resources from threats and breaches. As frontline defenders, the cybersecurity professional plays a vital, if not the most important role in protecting and ensuring the security of organizations' information resources. It is important to note that not all cybersecurity professionals are frontline defenders. Some are based on (a) building secure systems, (b) leadership and compliance, (c) operations (maintenance and recovery), while others are based on (d) defense (preventing, detecting, and responding), and (e) penetration testing (uncovering vulnerabilities) and cyber threat hunting.

[2] https://www.youtube.com/watch?v=G3Ep27sox7A

The last three categories may be considered frontline cybersecurity professionals since their main tasks involve uncovering vulnerabilities, preventing, detecting, and responding to an ever-shifting threat landscape (Assante and Tobey 2011; Hull 2017). The frontline defenders stand between cyber-adversaries and the organization, pushing back offensive attacks. Hence, cybersecurity burnout may vary depending on the extent to which the professional is engaged in cybersecurity frontline activities.

Burnout refers to a chronic response to job stressors characterized by emotional exhaustion, cynicism, and reduced self-efficacy (Maslach and Schaufeli 2001). The present study examines context-specific job characteristics associated with frontline defenders in order to understand why they experience burnout and how such burnout influences these cybersecurity professionals to leave the field, thus further contributing to job shortages. The information systems literature (Ahuja et al. 2007; Armstrong et al. 2015; Chen and Karahanna 2018; Moore 2000) offers a framework that helps us understand burnout in IS professionals in general. This literature ties together work load, job autonomy, fairness, role conflict, and their effect on work exhaustion, and ultimately turnover intention and work performance.

While the Maslach Burnout Inventory (MBI) scale can be used to measure the existence of burnout within the cybersecurity profession, not enough is known about this profession to be able to explain why or how the scale relates. In other words, there is scant research literature on the cybersecurity profession, and especially the frontline aspects of the profession. Although it has been adapted to studies in IS, the MBI scale was developed for and has been widely studied on professions that are dependent upon human services interaction (e.g., physicians, nurses, attorneys, educators). In contrast to the human services interaction, cybersecurity professionals work within a different context**.** In delving deeper into the contextual factors specific to cybersecurity job demands and workload, we propose our initial research questions: (1) *To what*

extent does the cybersecurity context (job characteristics) influence burnout in cybersecurity professionals? (2) To what extent is burnout different for frontline cyber-defenders versus other cybersecurity roles? While burnout, which is often characterized as work exhaustion has been adapted for IS professionals (Ahuja et al. 2007; Armstrong et al. 2015; Chen and Karahanna 2018; Moore 2000), we are unaware of theory-based empirical studies that have examined burnout in the context of cybersecurity professionals. This is a fundamental issue since the safeguarding of organization's resources (which can mean the success or failure of an organization) depends on the retention of a healthy cybersecurity workforce.

Further, Ahuja et al. (2007, p. 3) propose that the individual's role identity should have an effect on their perceptions and that the "*more salient the identity, the stronger its effect on perceptions*" of their job. *Identity* answers a fundamental question, "Who am I?" This question can be answered in relation to a person's social role including their professional role. Following the identity theory, we define cybersecurity role identity as a meaning attributed to oneself in relation to the cybersecurity role (Burke and Tully 1977). The notion is that when an individual's self-concept is wrapped around the roles they occupy, it influences their work. This notion is supported by calls for more research that explores the individual's role identity in understanding burnout and exhaustion in IS professionals (Armstrong et al. 2015). In heeding the call, we seek to examine how the contextual characteristics specific to cybersecurity job demands influence cybersecurity role identity and how this identity influences burnout. This prompts the research question: (3) *How does cybersecurity role identity influence burnout in cybersecurity professionals?*

By focusing on cybersecurity professionals, their role identity, and burnout, we draw attention to the important but rarely explored role of the population whose job is to defend organizations from cyber-attacks. The study seeks to contribute to the IS security literature by

examining a critical group of cybersecurity professionals, that to our knowledge, has not been studied. The study contributes by conducting an empirical study on a problem that could impact cybersecurity defenses as the threats and consequences of cyberattacks increase. With a better understanding of the cybersecurity profession and its increasing burnout phenomenon, effective solutions may be proposed and perhaps implemented by organizational cybersecurity and human resources managers to address the issue.

The remainder of the paper is organized as follows. We develop the cybersecurity context in order to understand the characteristics of this work. Then, we present the proposed conceptual model and propositions, proposed methodology, and expected results.

THEORETICAL FOUNDATION

Burnout is characterized by *exhaustion*, *cynicism*, and *self-efficacy* (Maslach and Schaufeli 2001). Exhaustion is the stress dimension of burnout and defined as the depletion of one's mental resources. Exhaustion is viewed as "the central quality of burnout and the most obvious manifestation of this complex syndrome" (Maslach and Schaufeli 2001, p. 402). Cynicism is a mental distancing, where individuals create a cognitive distance from their work as a way to cope with the deluge of work (Maslach and Schaufeli 2001, p. 403). Self-efficacy (or inefficacy) is the individual's feelings of effectiveness (or ineffectiveness) and productivity in their work. While IS studies have primarily focused on the exhaustion dimension of burnout and on an individual's overall career experience (e.g., Armstrong et al. 2015), the present study examines all three MBI dimensions. A review of the IS burnout literature provide differing results that requires more research. For example, Ahuja et al. (2007) finds that work overload, work-family conflict, fairness, and autonomy, affect exhaustion, which in turn affects turnover intention. Armstrong et al. (2015) finds that fairness, control of career, and workload affect exhaustion, however, exhaustion only influences turn-away intention through commitment to IS profession.

Rutner et al. (2008) also finds that workload, role conflict, and autonomy do not significantly affect exhaustion, which in turn does not significantly affect turnover intention.

In the study, we identify specific job characteristics of cybersecurity frontline defenders that present unique job demands when compared to other IS work. For example, work performed by cybersecurity professionals may be unique with respect to its secrecy, high visibility of failures, costly impact of failures, and the constant need for intense vigilance, speed and accuracy to thwart cyber attacks (Corman 2019; Dykstra and Paul 2018). Figure 1 presents an initial conceptual model on occupational burnout of cybersecurity professionals and its effect on cybersecurity work performance. The model reflects an understanding gained from extant research that burnout arises from antecedent beliefs of job (demand) characteristics (Maslach and Schaufeli 2001). According to Figure 1, burnout is expected to influence cybersecurity performance. Within a cybersecurity context, cybersecurity performance refers to the efficiency and effectiveness in which cybersecurity professionals engage in monitoring and defending the security of their organizations' resources. We also anticipate that cybersecurity role identity mediates this relationship.

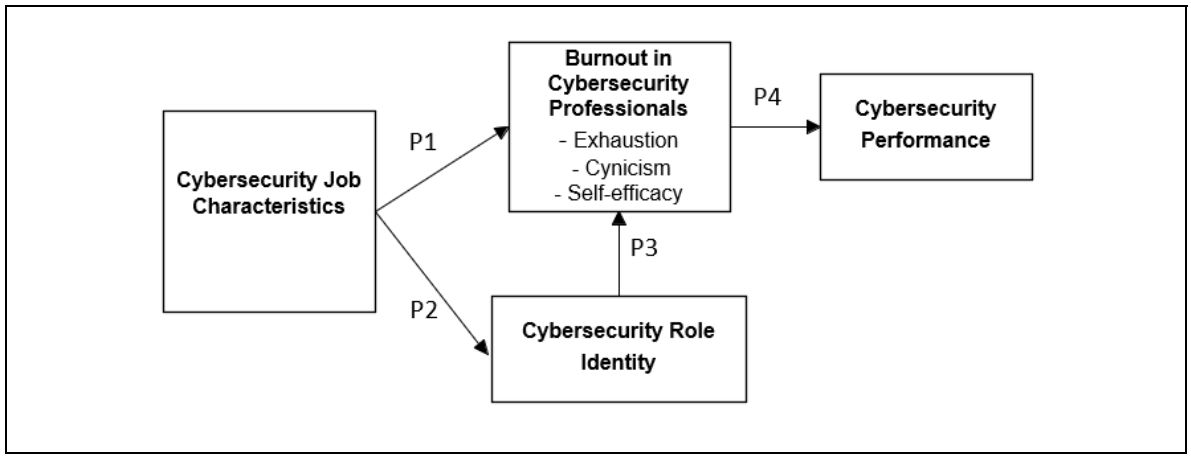

Figure 1: Proposed Conceptual Model

Often characterized as workloads exceeding human limits, job demands has been used consistently as a key contributing factor to burnout (Maslach and Leiter 2008). It is important to

note that excessive workloads do not necessarily lead to burnout if workers take time to recover. Excessive workloads become stressors and increase burnout when the workload is chronic and there are little or no opportunities to rest and recover from previous loads. In this study, the cybersecurity job context could be described as chronic. It is one where there are sustained attempts from countless cyber-adversaries from different time-zones and with different motives and tools trying to break organizations' security. It has been described as "*one of the only IT roles where there are people actively trying to ruin your day, 24/7*" (Schueler 2019). Hence, cybersecurity professionals in a context characterized with sustained cyber-attacks may experience burnout. In addition, we suggest that while burnout is applicable to cybersecurity professionals at large, the frontline security defenders may experience higher levels of burnout. For example, a failed security due to the unpredictable or evolving nature of vulnerabilities may suggest that the frontline defenders missed uncovering a vulnerability. Because these failures can be also be highly visible and publicized (e.g., Equifax breach), they could add to the job stressors. Thus, we suggest that frontline security defenders (e.g., ethical hackers) may be more susceptible to burnout than other security professionals (e.g., compliance, identity and access management), because of the characteristics of their jobs.

> *Proposition 1a: Cybersecurity job characteristics positively influences burnout in cybersecurity professionals*
> *Proposition 1b: Frontline cybersecurity job characteristics positively influences burnout in cybersecurity professionals more so than general cybersecurity job characteristics*

Cybersecurity role identity is a meaning attributed to oneself in relation to the cybersecurity role (Burke and Tully 1977). Generating a security role identity self-meaning is a sense making process that takes place when individuals perform role related activities. Role based experiences and activities should influence role identity. Verifying one's identity is the cognitive process through which individuals see themselves in terms of the social role (i.e., cybersecurity role) (Stets and Burke 2000). This means that past cybersecurity job characteristic behaviors (e.g.,

vigilance related monitoring), as seen by the self, should predict future behaviors as an individual tries to make their identity consistent with past role-related behaviors (Farmer et al. 2003). Previous studies have found support for the relationship between an individual's views of behavior and a related role identity. For example, Farmer et al. (2003) found that self-views of creative behaviors influenced creative role identity.

Proposition 2: Cybersecurity job characteristics positively influences cybersecurity role identity

An individual with a strong role identity continues performing role-based activities, because it is expected of them within their community (Stryker and Serpe 1982). Thus, a person with a strong cybersecurity role identity will continue to perform even when they may be emotionally or physically tired, because of the expectation of the role. Hence, we expect that an individual with a strong cybersecurity identity will experience increased burnout more so than a person with a low role identity. Previous research finds that an individual with a strong role identity experiences more burnout (Devery et al. 2018). Further, identity theory literature provides reasoning that role identity relates to one's self-efficacy. That is, to the extent that an individual has a salient role identity, the self-evaluation of their performance (self-efficacy) will be influenced (Burke and Stets 2009). Although burnout researchers have not integrated the self-efficacy dimension, identity theory suggests cybersecurity role identity influences the self-efficacy dimension of burnout.

Proposition 3: Cybersecurity professional role identity positively influences burnout in cybersecurity professionals

The burnout literature provides ample evidence of the effect of burnout on work performance and turnover intention (Ahuja et al. 2007; Armstrong et al. 2015). The notion is that when individuals feel exhaustion, cynicism, and reduced self-efficacy, their work performance reduces. A cybersecurity professional who is too exhausted and cynical about the job

characteristics that define their jobs, and who negatively evaluates their capabilities will begin to exhibit reduced performance in their security work. For example, this person may no longer devote the same level of effort at monitoring, defending, and safeguarding their organization's resources.

> *Proposition 4: Burnout in cybersecurity professionals negatively influences cybersecurity performance.*

METHODOLOGY

A multi-method study will be conducted to examine and expand upon the conceptual model. Interviews with approximately ten cybersecurity professionals will be conducted in order to identify their job characteristics, and to gain a greater understanding of how burnout is experienced in this profession, and its effects on cybersecurity performance. An initial qualitative study with interviews is needed in order to gain a greater understanding of context, including how to measure job characteristics, role identity, burnout, and cybersecurity performance for cybersecurity professionals. Indeed, separate MBI scales have been created for different professions, such as MBI for human services (MBI-HSS). It is anticipated that the MBI scale for cybersecurity professionals will differ from those applied to general IS professionals. Results from the qualitative study will subsequently serve as input into a refined theoretical model. A survey instrument will be developed in order to test the model across a larger sample of cybersecurity professionals, thus providing generalizability.

EXPECTED RESULTS

By drawing attention to the important but rarely explored role of cybersecurity professionals, their context-specific job characteristics, role identity, and burnout, we provide a better understanding of their role in cyber defenses, why they burnout, and add to the IS security literature.

REFERENCES

Ahuja, M., Chudoba, K., Mcknight, D. H., and George, J. F. 2007. "IT Road Warriors: Balancing Work-Family Conflict, Job Autonomy, and Work Overload to Mitigate Turnover Interntions," *MIS Ouarterly* (31:1), pp. 1–17.

Armstrong, D. J., Brooks, N. G., and Riemenschneider, C. K. 2015. "Exhaustion from Information System Career Experience: Implications for Turn-Away Intention," *MIS Quarterly: Management Information Systems* (39:3), pp. 713–727. (https://doi.org/10.25300/MISQ/2015/39.3.10).

Assante, M. J., and Tobey, D. H. 2011. "Enhancing the Cybersecurity Workforce," *IT Professional* (13:1), IEEE, pp. 12–15. (https://doi.org/10.1109/MITP.2011.6).

Burke, P., and Stets, J. E. 2009. *Identity Theory*, New York: Oxford University Press.

Burke, P., and Tully, J. 1977. "The Measurement of Role Identity," *Social Forces* (55:4), pp. 881–897.

Chen, A., and Karahanna, E. 2018. "Life Interrupted: The Effects of Technology-Mediated Work Interruptions on Work and Nonwork Outcomes," *MIS Quarterly: Management Information Systems* (42:4), pp. 1023–1042. (https://doi.org/10.25300/MISQ/2018/13631).

Corman, J. 2019. "Stress, Burnout and You: Fireside Chat with Dr. Maslach," *RSA*. (https://www.youtube.com/watch?v=G3Ep27sox7A&t=2s).

CSO. 2019. "5 Ways to Curb Cybersecurity Burnout | CSO Online," *CSO*. (https://www.csoonline.com/article/3387418/5-ways-to-curb-cybersecurity-burnout.html, accessed September 25, 2019).

Devery, H., Scanlan, J. N., and Ross, J. 2018. "Factors Associated with Professional Identity, Job Satisfaction and Burnout for Occupational Therapists Working in Eating Disorders: A Mixed Methods Study," *Australian Occupational Therapy Journal* (65:6), pp. 523–532. (https://doi.org/10.1111/1440-1630.12503).

Dykstra, J., and Paul, C. L. 2018. "Cyber Operations Stress Survey (COSS): Studying Fatigue, Frustration, and Cognitive Workload in Cybersecurity Operations," in *11th {USENIX} Workshop on Cyber Security Experimentation and Test*.

Farmer, S. M., Tierney, P., and Kung-Mcintyre, K. 2003. "Employee Creativity in Taiwan : An Application of Role Identity Theory," *Academy of Management Journal* (46:5), pp. 618–630.

Hull, J. L. 2017. "ANALYST BURNOUT IN THE CYBER SECURITY OPERATION CENTER-CSOC: A PHENOMENOLOGICAL STUDY."

Indeed. 2019. "Global Cybersecurity Outlook 2019 - Indeed Blog," *Indeed.Com*. (http://blog.indeed.com/2019/04/25/cybersecurity-outlook-2019/, accessed September 16, 2019).

Kappelman, L., Torres, R., Mclean, E., Maurer, C., Johnson, V., and Kim, K. 2018. "The 2018 SIM IT Key Issues and Trends Study," *MIS Quarterly Executive* (18:1), pp. 237–263.

Maslach, C., and Leiter, M. P. 2008. "Early Predictors of Job Burnout and Engagement," *Journal of Applied Psychology* (93:3), pp. 498–512. (https://doi.org/10.1037/0021-9010.93.3.498).

Maslach, C., and Schaufeli, W. 2001. "Job Burnout," *Annual Review of Psychology* (52), pp. 397–422.

Moore, J. E. 2000. "One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals," *MIS Quarterly* (24:1), Minneapolis, p. 141.

Morgan, S. 2017. "Cybersecurity Jobs Report 2018-2021," *CyberSecurity Ventures*. (https://cybersecurityventures.com/jobs/, accessed September 16, 2019).

Reid, D. 2019. "DAVOS WEF," *CNBC*. (https://www.cnbc.com/2019/01/18/recession-is-the-number-one-fear-for-ceos-in-2019-survey-says.html, accessed September 16, 2019).

Rutner, P. S., Hardgrave, B. C., and McKnight, D. H. 2008. "Emotional Dissonance and the Information Technology Professional," *MIS Quarterly* (32:3), pp. 635–652.

Schueler, C. 2019. "Why Cybersecurity Burnout Is Real (and What to Do ...," *DarkReading*. (https://www.darkreading.com/threat-intelligence/why-cybersecurity-burnout-is-real-(and-what-to-do-about-it)/a/d-id/1333906, accessed September 17, 2019).

Stets, J. E., and Burke, P. 2000. "Identity Theory and Social Identity Theory," *Social Psychology Quarterly*, pp. 224–237.

Stryker, S., and Serpe, R. T. 1982. "Commitment, Identity Salience, and Role Behavior: Theory and Research Example," in *Personality, Roles, and Social Behavior*, New York, NY: Springer New York, pp. 199–218. (https://doi.org/10.1007/978-1-4613-9469-3_7).