Job Stress in the Cybersecurity Incidence Response Work Role

Janine L. Spears, *DePaul University*

Abstract

An exploratory study was conducted to examine job stress in the cybersecurity workforce. Interviews with fourteen cybersecurity professionals provided rich contextual descriptions of their typical work day; what they like most about their jobs; the extent to which they experience job stress; the sources of their high or low self-reported stress levels; and the impacts they have experienced. Study findings suggest that high levels of job stress inherent in the incidence response (IR) work role is a contributing factor to the skill shortage in the "protect and defend" cybersecurity work category defined by the U.S. NICE. Job stress factors were identified in IR work. Finally, the study concludes with recommendations on how to reduce job stress for IR workers. The aim is to reduce job turnover in the IR work role and thus retain a sought-after skillset that informants consistently indicated takes several years to build.

1. Introduction

People are key assets in protecting cybersecurity, yet cybersecurity workforce shortages persist [1]. There are estimates of a 3.4 million global cybersecurity worker shortage, including a 410,000 gap in the United States [2]. Moreover, the cybersecurity labor market often lacks the desired skillset or skill level to effectively combat evolving cyber threats [1, 3]. Intuitively, it is important to keep existing skilled cybersecurity workers given that the skillset takes years to develop.

However, as security threats continue to increase while internal security teams remain under-staffed, job-related stress takes hold. There are accounts of relatively high turnover in internal security departments in jobs. Moreover, burnout was a keynote topic at a major cybersecurity industry conference [4], suggesting that daily security work is stressful. There is an established body of research linking job stress to employee turnover in various professions, including IT workers in general [5-8]

Workshop on Security (and Privacy) Information Workers (WSIW 2023) at the USENIX Symposium on Usable Privacy and Security (SOUPS) 2023. August 6 - 8, 2023, Anaheim, CA, USA.

There is limited academic research on cybersecurity workers. Moreover, extant cybersecurity workforce literature has largely focused on skill shortage and training within the profession. However, given that job stress is expected to lead to worker turnover, research is needed on job stress in security work. Consequently, the present study examines stress factors in cybersecurity work. An exploratory study was conducted that involved nearly 1000 minutes of interviews with cybersecurity workers. The research questions examined are:

1. Is job stress widespread across security work roles?
2. What contributes to job stress in security work?
3. What are the effects of job stress?
4. How might job stress be reduced?

2. Literature Review

Prominent industry studies consistently report a major shortage in the cybersecurity workforce and the skillset needed to defend against ever-evolving cyber threats [2, 9]. A consensus that a worker and skill gap exist has prompted a growing body of literature examining innovative pedagogical tools to improve learning outcomes in cybersecurity education [10-12]. Research has also examined the requirements included in cybersecurity job postings across specialty areas as a means to inform educators with the aim of closing the skills gap [1]. Finally, self-determination theory has been examined as a means to cultivate cybersecurity learning [13].

The present study is distinguished from and builds upon this literature by examining job stress as a potential means to reduce worker turnover. Extant research has found burnout among IT workers leads to lower job satisfaction and higher job turnover [5, 6]. The author is unaware of an empirical study that examined job stress or burnout among cybersecurity workers. Thus, the present study makes a contribution to the cybersecurity workforce literature by examining job stress from daily work in the profession.

3. Research Methods

An interpretive research approach was chosen in order to provide rich context that enables researchers to learn more about the work that security workers do, and where within that context they experience work-related stress. Such contextual insight is necessary since studies on job stress tend to focus on a particular profession. Therefore, any effective study on worker stress or burnout among security workers necessitates an understanding of the profession; what their day-to-day

work entails; challenges they face; and how that impacts their job stress. Moreover, the security profession has a myriad of different job roles. Thus, some understanding of the sub-contexts among different security jobs is helpful in interpreting study outcomes.

3.1. Interview Data Collection

The study obtained university IRB approval prior to data collection from human subjects. Semi-structured interviews were conducted with fourteen security professionals for an average of one hour each in duration. Prospective informants were recruited at an annual security conference where the researcher distributed a flyer inviting security workers to participate in the study. The researcher also contacted and invited security professionals previously met at other security events, each of whom had different types of security jobs and varied in their years of security experience. Prospective participants were told the study aimed "to understand the unique work demands and their effects on security workers responsible for identifying cyber threats and preventing attacks." Each interview began with the researcher stepping through an IRB-approved consent form. Informants were told that they could skip any questions they were not comfortable answering; that their identities and that of their employers would remain anonymous. Informants provided explicit consent.

Study informants included six females and eight men; eight senior security professionals (>= 10 years), five mid-level (3-9 years), and one early in the profession (<= 2 years). Nine of the informants worked for an internal security department tasked with protecting the security of their organization's systems; four worked externally as consultants. One person worked within an internal security department the year prior to the interview and then switched to work as a consultant. He gave accounts from both perspectives of working internally versus now working as a consultant. A variety of job roles were included in the study: security analysts; security architect; governance, risk management, and compliance (GRC); penetration testers; and security leadership. One informant left the field from job stress and shared what led to her exit.

Informants in an incident response (IR) role tended to be in the early or mid-career stage in security. Informants working in the senior management category had more than 10 years of security work experience and led an internal security team. Informants working in a GRC role most often worked on regulatory compliance. However, this role can also include risk management, audit, and security policy development.

Each informant worked for a different organization. Informants working in IR, GRC, or senior management roles worked within a company and are considered "in-house" security, meaning their security work is for the protection of their employer's network, data, and systems. In contrast, the consultant category refers to security workers who provide billable security services for external clients. Informants who were consultants tended to work as pen testers or perform technical compliance audits.

An interview script served as a guide to ask each informant a base set of questions. An excerpt is provided in the Appendix.

3.2. Interview Data Analysis

This study was exploratory in that the purpose was to discover, as opposed to testing theory on, daily work and stress in the cybersecurity workforce. Interview data were transcribed into text. Interpretive analysis was conducted using an iterative process of reading informants accounts; identifying key words and themes that emerged as salient across interviews; and making causal connections [14, 15].

For example, each IR informant used the word and discussed "alerts." Sentences on "alerts" were analyzed across accounts on IR work. A theme clearly emerged that alerts are voluminous. Informants were asked what they liked most about their work; then, what they liked least. A common theme emerged across interviews that responding to alerts is challenging in two ways: intellectually stimulating (what they like most) while also being draining (what they liked least). When asked to describe the cause of their work stress, common themes emerged across IR informants' accounts (e.g., sense of responsibility; sense of urgency; small work group; etc.)

The researcher's interpretation of qualitative results is assessed as part of a multi-method study. That is, the results of the present study served as input into a positivist study for theory testing using a survey instrument and structural equation modeling. That study is in-progress.

Common themes that emerged across interviews formed the basis of the stress factors described in the next paper section. Pseudonyms are used in place of informants' names in order to protect their and their organizations' identities.

4. Results

It became clear early in the data collection that informants working in incidence response experienced high degrees of job stress relative to other security work roles in the study. Four of the six informants who worked in incidence response switched to what they each described as a less stressful role – either in an internal GRC job, or as an external consultant. Three of the four informants who made the switch explained that they did so, because they wanted a less stressful job. One IR informant was promoted; another IR informant indicated preferring e-discovery work. Two of the three informants who made the switch to reduce stress did so within the first 2-3 years of their security careers.

Informants were asked to rate their job stress level on a scale of 1 to 5, with 5 being the highest. Informants working in IR and those in internal security leadership roles consistently rated their stress levels at a 4 compared to those working in consulting and GRC roles rating theirs at 2. Informants who switched from an IR job to GRC or consulting jobs reported their stress level changing from 4 to 2 after the switch.

Based on these findings, the remainder of this paper focuses on IR workers -- one of the two security job categories that self-reported the highest degree of job stress when compared to other job categories included in the study. Next, IR work is described based on NICE [16] and informant testimony.

4.1. What is a Cyber Security Incident Responder?

The incident response work role is part of the Protect and Defend cybersecurity workforce category [16]. In general, a cybersecurity incident responder (IR) "investigates, analyzes, and responds to cyber incidents within the network environment or enclave" [17: p. 14]. Depending on an organization's structure, some of the incident responders in the present study also worked in additional roles, such as cyber defense analysis (i.e., collecting data from a variety of enterprise security software logs to analyze threats) and cyber defense infrastructure support (i.e., testing, implementing, maintaining, and administering enterprise security hardware and software infrastructure).

IR workers are the frontline defense of an organization's security. When they receive alerts on anomalous system behavior or traffic, it is their job to quickly discern the extent to which the alert is a serious threat and most often, to resolve the alert. The next section describes an IR's typical work day.

4.2. A Day in the Life of an Incident Responder

Inherent in IR work is responding to system alerts. Informants working in IR described a typical day beginning with checking for and processing security alerts that may have occurred overnight. The alerts are typically auto-generated from security software, including email alerts; Microsoft 365 Defender alerts; firewalls, incidence response systems, and other enterprise security systems. Kathy's account was very similar to the other IR informants:

> First thing I do when I come in in the morning is to check the emails for the IT security email box[...]. I look at any alerts that came in overnight, and especially the high-level alerts, I do triage on those.

The time it takes to handle alert depends on the particular alert. When asked the average time it takes to resolve an incident, one informant explained:

> It depends on what it is. You get small ones and then you get some big ones that can take weeks.

Another informant did not report voluminous alerts at his organization as other informants recounted. Nonetheless, his work day also started with checking for and resolving alerts. He was asked the average time it takes to resolve incidents:

> [...] even a 9:00 AM incident, Monday morning incident response project basically would derail the whole day, if you're lucky. If not, it would take more.

Manny described the types of systems he received alerts from while in his IR work; the number of network endpoints he was responsible for monitoring daily; and the basic process for handling each alert:

> [...] I was basically monitoring near about 5,000 endpoints and it was a lot. So, the email firewall, the EDR [Enhanced Detection and Response], the [inaudible] system, everything fell up to the security guy. […] There are way too many alerts flying around and all those alerts are ticketed. All the tickets have a certain time when they need to be addressed; otherwise, they're escalated automatically by a ticket system. So, there's a lot going on and for resolving some issues, it also depends on how your security department is structured.

Delia's role was to investigate security alerts and then design and build programming code to automate a response to common types of alerts, as described:

> I do automation development, right? So, I try to work ahead of the attack. So really, we do a lot of our own research of, okay, what have we seen in the company history? Right. So, what is our biggest vulnerability? We prioritize those. And then, how can we automate what our process is right now? And then, I'm working daily to automate those processes, whether or not we're getting attacked.

In addition to handling alerts as they arise, IR workers reported researching new security solutions. Several IR informants highlighted the importance of their building relationships with other IT groups and with business users in order to diplomatically gain acceptance of needed security improvements. In cases where an organization's security group is short-staffed, the IR worker may also perform additional roles, such as monitoring security screens in a SOC (Security Operations Center). For example, "Tommy" worked with his direct-report and the two comprised the core security group for a large organization:

> So "John" and I pretty much did all of it including monitoring. It's sad to say it, but we were eyes on screens, we used Splunk as the SIEM [security information and event management system] and we would set up dashboards and alerts based on anomalous stuff. […] John and I get alerts at all times of the day, and whether or not we are available dictates whether or not there is a response.

4.3. Stress Factors in Incidence Response Work

Stress factors were revealed during informant accounts of their daily work. In addition, informants were asked the source of their self-reported job stress level. Three salient stress factors that emerged included (a) the weight of responsibility on IR workers' shoulders to detect a potential cyber intrusion; (b) the volume of alerts, sense of urgency to resolve alerts, and the shortage in labor to help manage the load; and (c) the difficulty in mentally unplugging from work. Each of these stress factors is described next.

4.3.1. The Weight of Responsibility

IR workers consistently described a sense of responsibility in their defender work role as a source of job stress. For example, informant "Jerry" stated that incidence response was stressful. He was asked what was the stressful part:

> Well, I guess knowing the responsibility of being the responsible party for the client information, knowing that we would have to send the breach notification letters, go on the CMS wall of shame. It was a heavy responsibility. […] I think when you internalize that and take that responsibility seriously, it can be very stressful.

"Carl" is a senior consultant with 20+ years of security experience. The past 10+ years, he's been an application pen tester for large organizational clients' software. He rated his work stress level as a 2 out of 5. Carl explained his low stress level in comparison with internal security defenders:

> So, my job is to break stuff. My job is to pen test. My job is to identify vulnerabilities in my customer's products. My job is not to defend. [Conversely, if] my job is to make sure all of our security systems and things are working to defend us against attack. That's stressful. That's hard.

4.3.2. Alert Volume, Urgency, and Labor Shortages

Informants working in internal security groups commonly indicated their IR operation was short-staffed. For example, one informant worked in a group of 2 to handle security alerts within an organization that had a complex user base of over 25,000 users; various enterprise software; and an extensive network. In addition to IR work, this 2-person team also performed SOC monitoring; and they requested, planned, designed, developed, implemented, and maintained enterprise security technology solutions.

In another example, Manny indicated he worked on a "really small" security team for a regional retailer with brick-and-mortar and electronic stores. There was time pressure to handle a high volume of alerts, resulting in job turnover.

> [...] there was a lot of work because our team was really small and I was basically monitoring near about 5,000 endpoints and it was a lot. We had a lot of turnover at my previous job. So, at some point it got really hard because you can't really take any of the platforms offline.

A third informant's account described a labor shortage:

> [...] we always had a small team to work with as well. So it wasn't just me, it was the team as well working. We just didn't have enough of us. And then people leave and then it's hard to find people to fill those roles as well that have the experience.

4.3.3. Difficulty Mentally Turning Off Work

One informant who worked for a very large manufacturer described how her work interfered with life off-hours:

> You're always on alert. You're always on call. And during the holidays, it's usually one of the worst times: there's always an incident of some sort that happens. So, you never have a break from it. A holiday is never a holiday. So, when I was the team lead, we were always responding, we were always working. Even when we were supposedly closed [...]. So even on, like I said, on the holidays, Memorial Day, July 4th, Christmas, New year's, we were always working. Someone was always on call. We just never received a break.

Similarly, another IR informant working for a multi-national manufacturer further explained that: "Attacks definitely increase during the holiday season, for sure."

Informants were asked their average work hours per week. Similar to other informants, one person explained that it is difficult to estimate work hours, because even when he is not technically at work, he is unable to "unplug" from work:

> It's hard [to say] because it's hard for me to unplug [...] We've got technology on our wrists, and it's hard to unplug. I've even gone through the privacy settings and said, "Don't notify me." But you can't help but see that red bubble badge that shows one message in Teams or Outlook or whatever, and not actually look at it. And when you're in security you have this inherent ownership, you feel like there's a lot of weight on your shoulders and you don't want to miss something. Because a lot of what we do and how much work we have to put in when there is an incident is very heavily dependent on how quickly we would react to it.

4.4. Impacts of Job Stress in IR Jobs

Informants were asked how they experience job stress. Restless sleep and occasional mistakes on the job were cited. There was also evidence of job role turnover.

4.4.1. Sleep Loss and Restlessness

Informants reporting high job stress described stress impacting their sleep. For example, when asked how he experiences job stress, Tommy responded:

> So, sleep for sure, tossing and turning thinking about work, that's probably the most predominant one.

Another informant recounted sleep loss as a stress impact:

> I would say sleeping and being tired, because you would get called at all hours. And you might have a long day, you've worked all day and you might work a 14-hour day, a 12 or 14-hour day and you think, okay, I'll get some sleep, and then an incident happens. And then you're up and you might be working those hours for several days. [...] So you're mentally and physically exhausted.

4.4.2. Worker Turnover in IR Jobs

Work role turnover was a salient finding among informants who transitioned out of IR work into what they described as less stressful roles in GRC or consulting.

One informant illustrates this trend among study participants. He began his career working as a pen tester for a small security company. He wanted to gain experience working for a larger company so took an IR job within a small internal IT security department. After 2.5 years, he left his IR job and switched to a consulting role where he now performs pen testing and compliance audits for clients. He rated his stress level at 4 while working in IR; in contrast, he says his stress level dropped to 2 when he transitioned to an external, consulting job. He described his experience working in an IR role that ultimately prompted him to transition out:

> It got really overwhelming and I mean, at one point of time, you just cannot function properly. There's just so much of stuff happening. It gets really hard to prioritize things. And I think you are not as productive as you want to be. I think that's how I experienced it. So, I talk to my CISO at that point in time and tell him, "I need a few days off."

Another informant, Jerry, began his security career after working in IT for over 10 years in various roles. His first security job was in an IR role. After 2.5 years, Jerry left his IR role and employer to transition to leadership role in managing IT services. While Jerry says he found his previous security role to be very interesting, the amount of work, degree of responsibility, and job stress spilled over into his family life prompting him to make a career change to a general IT leadership role with some GRC responsibility.

4.4.3. Lapses in Job Performance

Multiple IR informants hinted at lapses in job performance when job fatigue sets in. As one person explained:

> Easier to make a mistake, more chances that I will not be listening, just because of how many times I'll be zoned out, which is horrible.

4.5. What Attracts IR Workers to Stay in Spite of High Stress

The challenge of the work and the workday being different each day (not dull) were the top two reasons cited for what informants liked most about their work. Similar to the challenge was the notion of problem-solving -- having to figure out the problem and a solution, with each problem being something different. As one informant put it, “incidents are kind of fun” – meaning, a problem to investigate and solve. Change is inherent in the job role, because the problems change. Finally, team collaboration among IR workers was also cited as what they enjoyed most about their jobs.

4.6. Stress Reduction Mechanisms Informants Use or Suggest

One informant recounted informal “therapy sessions” among security peers who worked for the same organization. They would go to lunch or grab a beer at a local watering hole. Therapy sessions were later extended to include security peers working within the same industry. Therapy sessions were initially used to blow off steam, but as the sessions grew with more workers, they were used to share security tips on how to respond to various types of incidents. They also provided an informal support system among workers with like-experiences, including job stress, in their line of work.

When asked how IR work could be made less stressful, Tammy suggested organizations invest in more labor:

> I think having more resources. I think companies just don't have enough people to do the work. [...] I think that's the biggest thing, is not putting money into the people as well. You do see companies put money into tools. But you'll also need people to be managing and looking and handling those tools. And if you don't have that, again, they'll get burnt out.

5. Discussion

Fourteen cybersecurity workers were interviewed in order to gain a greater understanding of the type of work they do; to what extent they experience job stress; and contributing factors to their job stress level. Among the study informants interviewed, stress was reported at significantly higher levels for in-house security workers in IR when compared with GRC work and external consultants.

A key stress factor in IR work is the weight of responsibility on their shoulders to effectively handle security alerts in order to prevent or quickly detect a cyber attack. The responsibility stressor is exacerbated by high alert volume, a sense of urgency, and labor shortages. IR informants described a persistent anxiety that they may miss some important technical detail that enables an attack to occur, or that they may be busy with other tasks and be too slow to notice a cyber attack before significant damage is done to their organization or end users. Consequently, IR workers find it difficult to unplug from handling or anticipating alerts. Thus, even when an IR worker is not physically on the job, they are mentally on alert.

The high stress over time resulted in several former IR workers in the study transitioning to less stressful job roles, thus exhibiting a form of job turnover. These findings are

consistent with the job burnout literature that predicts high levels of job stress (or worker burnout) to increase job turnover [5, 7]. IR workers more technologically-focused transitioned to pen testing or auditing as consultants, while the others transitioned to GRC roles.

The problem with this career trajectory is that IR workers build up strong technical skills over the course of years analyzing and resolving alerts, but then leave the IR role when they burn out, resulting in a skill loss to the "protect and defend" security work category. It then takes years for the security team left behind to find and train the next IR worker to have the skill level of the person who left the IR role to transition to a different, less stressful security role. This finding accounts for one important reason why there is gap in security skills within the IR work role.

5.1. Research Implications:

Study findings suggest that high levels of job stress inherent in the IR work role is a contributing factor to the skill shortage in the "protect and defend" work category, as defined by NICE [16, 17]. Organizational investment in stress-reducing mechanisms for IR work may result in fewer IR workers leaving the role. Intuitively, the fewer IR workers exiting the role, the more IR skill retained in this critical work function.

5.2 Recommended Future Research on Stress Reduction

The present study found the sheer number of alerts, the complexity of handling some alerts in a timely fashion, and the sense of urgency to promptly address each alert can be stress-inducing for IR workers. Moreover, enterprise security systems often produce a high degree of false-positives and tend to provide insufficient information for alert analysis [18, 19]. Novel automated methods for reducing the rate of false-positives and improving the quality of security alerts [18, 20] can provide relief to IR workers. In addition, better processes are needed for manual assessment of security alerts. Given the fast-paced evolution of security threats, a holistic approach to alert analysis is recommended. For example, improvements in cognitive approaches to analyzing alerts more efficiently [21] may reduce work stress. Case study research is needed to pilot cognitive frameworks for conducting alert analysis within IR work groups.

A sense of responsibility was found to be a major stress factor for IR workers. Given that IR is classified as a "specialty area" within the security workforce [16, 17], there may be limited opportunity to redistribute IR work. However, one potential means of reducing work stress is to redistribute the weight of responsibility for security incidents to other roles within the IT organization and business leadership. For example, one IR informant stated he would "feel a lot better and less responsible" if organizational leadership would agree to implement a major security mechanism that was missing and left a glaring security vulnerability in access control. Senior security managers described frustrations with a lack of business buy-in on needed security processes. Organizational governance research is needed on formal mechanisms to effectively distribute responsibility for security incidents across security, other IT, and business roles.

Informants described small, under-staffed, IR work groups. Frameworks defining security job functions are helpful in understanding the scope and distinctions among various types of security roles [16, 17]. Research is needed on workforce allotment across security work roles to understand security staffing, including whether IR work groups tend to be relatively understaffed in internal security departments.

Given informant accounts of the difficulty in unplugging from work, coupled with accounts of poor sleep quality, an employee wellness program (EWP) tailored to reduce IR work stressors is recommended. There is a rich body of literature examining the effects of EWPs on employee productivity and healthcare costs [e.g., 22, 23, 24]. There is evidence that employee wellness interventions can reduce worker stress and fatigue when tailored to address its source [25]. Reductions in perceived stress and increases in job role retention are desired EWP outcomes to measure for IR workers.

5.3. Study Limitations

Study informants were recruited from cyber security conferences and affiliated professional associations. The pool of participating applicants did not include security roles, such as security analysts working on identity and access management; SOC analysts; etc. Findings from the present study are not necessarily generalizable to the broader security profession. Therefore, results from this qualitative, interpretive study serve as input into a subsequent positivist study where theory testing is being performed from a larger pool of respondents to a survey instrument; thus, enabling greater generalizability. Survey data collection is in-progress to test an adaptation of Maslach's Burnout Inventory theory [26, 27].

6. Conclusion

Security workers in incident response experience high degrees of stress from daily security alerts, time pressure, and a sense of responsibility to save their employer and users from a data breach. The results of this study found a trend in security workers leaving the much-needed role of incidence response and instead changing to the less stressful roles of GRC or consulting. Consequently, as more security defenders are needed, organizations are losing them. A concerted effort is needed by organizations to create institutional mechanisms that reduce the stress of this critical cybersecurity work specialty.

References

1. Ramezan, C.A., *Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field.* Journal of Information Systems Education, 2023. **34**(1): p. 94-105.

2. (ISC)2, *Cybersecurity Workforce Study*. 2022, (ISC)2. p. 86.

3. Wamsley, L., *CYBER SKILLS GAP WIDENS: Education is needed to build competencies as threats rise.* Internal Auditor, 2020. **77**(5): p. 13-14.

4. Corman, J., *Stress, Burnout and You: Fireside Chat with Dr. Christina Maslach*, in *RSA Conference Keynote*, C. Maslach, Editor. 2019, RSA Conference.

5. Moore, J.E., *One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals.* MIS Quarterly, 2000. **24**(1): p. 141-168.

6. Shih, S.-P., et al., *Job burnout of the information technology worker: Work exhaustion, depersonalization, and personal accomplishment.* Information & Management, 2013. **50**(7): p. 582-589.

7. Armstrong, D.J., N.G. Brooks, and C.K. Riemenschneider, *Exhaustion from Information System Career Experience*
Implications for Turn-Away Intention. MIS Quarterly, 2015. **39**(3): p. 713-728.

8. Chong, V.K. and G.S. Monroe, *The impact of the antecedents and consequences of job burnout on junior accountants' turnover intentions: a structural equation modelling approach.* Accounting & Finance, 2015. **55**(1): p. 105-132.

9. Suby, M., *The 2013 (ISC)2 Global Information Security Workforce Study*, in *A Frost & Sullivan Market Study* 2013. p. 26.

10. Hamman, S.T., et al., *Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students.* IEEE Transactions on Education, 2017. **60**(3): p. 205-211.

11. Yamin, M.M. and B. Katt, *Modeling and executing cyber security exercise scenarios in cyber ranges.* Computers & Security, 2022. **116**: p. N.PAG-N.PAG.

12. Sharevski, F., P. Treebridge, and J. Westbrook, *Experiential User-Centered Security in a Classroom: Secure Design for IoT.* IEEE Communications Magazine, 2019. **57**(11): p. 48-53.

13. Kam, H.-J., et al., *Cultivating cybersecurity learning: An integration of self-determination and flow.* Computers & Security, 2020. **96**: p. N.PAG-N.PAG.

14. Miles, M.B. and A.M. Huberman, *Qualitative Data Analysis*. 2nd ed. 1994: Sage.

15. Urquhart, C., *An encounter with grounded theory: tackling the practical and philosophical issues*, in *Qualitative Research in IS: Issues and Trends*, E.M. Trauth, Editor. 2001, IDEA Group Publishing: Hershey, PA. p. 104-140.

16. NIST, *Workforce Framework for Cybersecurity (NICE Framework)*, R. Petersen, et al., Editors. 2020, U.S. National Institute of Standards and Technology.

17. Management', U.S.O.o.P., *Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring and Retaining a Federal Cybersecurity Workforce*. 2018, U.S. Office of Personnel Management. p. 52.

18. Bryant, B.D. and H. Saiedian, *Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model.* Computers & Security, 2020. **94**: p. 1-23.

19. Alahmadi, B.A., L. Axon, and I. Martinovic. *99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms*. in *USENIX Security Symposium*. 2022. Boston, MA: USENIX Association.

20. Park, H. and Y.-J. Choi, *Frequency-Based Representation of Massive Alerts and Combination of Indicators by Heterogeneous Intrusion Detection Systems for Anomaly Detection.* Sensors, 2022(22): p. 1-15.

21. Andrade, R.O. and S.G. Yoo, *Cognitive security: A comprehensive study of cognitive science in cybersecurity.* Journal of Information Security and Applications, 2019. **48**: p. 1-13.

22. Gubler, T., I. Larkin, and L. Pierce, *Doing Well by Making Well: The Impact of Corporate Wellness Programs on Employee Productivity.* Management Science, 2018. **64**(11): p. 4967-4987.

23. Otenyo, E.E. and E.A. Smith, *An Overview of Employee Wellness Programs (EWPs) in Large U.S. Cities: Does Geography Matter?* Public Personnel Management, 2017. **46**(1): p. 3-24.

24. Smidt, M.N., et al., *Wellness programs and employee outcomes: the role of HR attributions.* Asia Pacific Journal of Human Resources, 2022: p. 1.

25. Biman, S., et al., *Effects of yoga on stress, fatigue, musculoskeletal pain, and the quality of life among employees of diamond industry: A new approach in employee wellness.* Work, 2021. **70**(2): p. 521-529.

26. Maslach, C., W.B. Schaufeli, and M.P. Leiter, *Job Burnout.* Annual Review of Psychology, 2001. **52**(1): p. 397-422.

27. Schaufeli, W., et al., *Maslach Burnout Inventory -- General Survey (GS)*. Vol. 31. 1996.

Appendix: Interview Script Excerpt

1. How long have you worked in the cybersecurity field?
    - In what industries?
2. What job titles have you held in the cybersecurity field?
3. What is the scope of your work role?
4. Describe a typical day at work in your security role.
5. What aspects of your security work do (did) you like most? Why?
6. What aspects of your security work do (did) you like least? Why?
7. Do (did) you experience stress from your cybersecurity work?
    - If so, to what degree on a scale of 1-5 where 5 = a great deal of stress; 1= no stress; 2= minimal stress 3= occasional stress; and 4= significant stress
8. What is (was) the source or cause of your work stress being at that level? (whether high or low stress)
9. In what ways do (did) you experience work-related stress? (This question is asked if informant expressed higher degrees of stress.)
10. Do you have any intention to leave the cybersecurity field? (Sometimes this was asked; other times, interviewees proactively stated they would not want to work in another field.)