Am I hired as a Firefighter? Exploring the role ambiguity and board's engagements on job stress and perceived organizational support of CISOs

Anna Piazza
School of Business, Operations and Strategy
University of Greenwich
London, United Kingdom
anna.piazza@greenwich.ac.uk ORCID: 0000-0002-5785-6948

Srinidhi Vasudevan
School of Business, Operations and Strategy
University of Greenwich
London, United Kingdom
srinidhi.vasudevan@greenwich.ac.uk
ORCID: 0000-0002-8584-9112

Madeline Carr
Department of Computer Science, Operations and Strategy
University College London
London, United Kingdom
m.carr@ucl.ac.uk ORCID: 0000-0001-6666-0595

Abstract - The role of the Chief Information Security Officer (CISO) in an organization is critical as they play a huge part to ensure business continuity and defend against the evolving threat landscape. Their role cannot be downplayed, especially in a context where new demands are imposed on organizations to defend their organizational boundaries against any cyber threats. As such, the job role is continuing to mature and the boundary of their role and responsibilities within the organization is challenging to define. Sometimes, there is a lack of clarity on the CISO's responsibilities. While studies look at managers' job stress, there is a dearth of research in the cybersecurity domain on role ambiguity's impact on job stress among cybersecurity professionals and how board engagement impacts perceived organizational support. Bridging this gap, this research uses primary data that has been collected from 24 CISOs from varied UK business sectors through semi-structured interviews to explain which factors are pivotal while looking at perceived organizational support and job stress. Our study sheds light on how role ambiguity contributes to job stress while perceived organisational support seen as better engagement of the board through cyber communication mitigates job stress. When these factors are understood, organisations can have better support mechanisms that will ensure that CISOs are well equipped to take on the cyber challenges while ensuring the organization's digital assets are protected.

***Keywords* -** CISO, cybersecurity, perceived organizational support, job stress, qualitative data.

1 Introduction

In organizations, cybersecurity operations ensure adequate practices are in place to secure systems, information, networks and other digital assets are protected from theft, manipulation, unauthorized access or other forms of exploitation. As such, it protects the organization and ensures business continuity [1]. The cyber threats that organizations face are growing significantly from ransomware attacks, phishing scams as well as direct, targeted attacks that are hostile and against critical infrastructure [2]. In a recent Global Risks Report in 2019, the World Economic Forum has placed cyber risk as a key global risk next to climate change showcasing the salience and the notoriety of cyber threats [3]. The severity of the cyber threats has been exacerbated by the COVID-19 pandemic and since then, there has been an increase in the sophistication as well as the number of cyber-attacks. This is evident in what can be called as a "Cyber Pandemic" during 2021 [4]. These trends showcase a huge challenge that the cyber domain often fails to address: the people [5]. The working environments for cybersecurity professionals often require multifaceted skills including creativity, problem-solving, memory and ability to be highly vigilant [6]. Stress impairs these skills, the cognitive abilities, effectiveness of individuals to carry out their tasks and their overall wellbeing. There have been studies that focus on burnout, fatigue and stress to some extent in cyber security operations [7], however, there is not much attention in the Information Systems/Security (IS) literature to specifically focus on the Chief Information Security Officers (CISOs) or those that are in the 'firing line'. At an organizational level, CISOs oversee operations and processes pertaining to securing the cyber and technological space. Given their role in ensuring the organization's digital assets including its critical information are secured and protected, they are also held responsible and liable when there are adverse cyber incidents that impact the organization. While this might be true for all C-suite positions, the CISOs are limited in their ability to respond to these threats in relation as it is intricately tied to the level of organizational resilience. This has an impact on how they experience their work environment, their job as well as the organizational support. Job stress is a notion that refer to how employees feel about their work environment [8]. The notion of perceived organizational support refers to the perception that the employee has about the extent to which their wellbeing is prioritized and how their contributions are valued by the organization [9]. Thus, when the organizational values, employees' expectations and feels are mismatched, this leads to an increase in the levels of stress the employees face, thereby prompting them to leave the IT profession [10]. As such, there could be crucial organizational, role-related and managerial aspects like board communication dynamics and role ambiguity that can be stressful, exhausting and taxing. However, little is known about how cyber managers perceive support from their organizations and their feelings towards their work. Moreover, in the information system field, aspects of human stress are ill-researched [11, 12] and there is a huge focus of looking it from a quantitative perspective or from the technology perspective of dealing with cyber threats. Against this background, we conducted 24 semi-structured interviews with CISOs from varied industrial sectors in the UK to investigate the following research questions:

i. What are the driving factors that impact job stress among cybersecurity professionals?
ii. How do cybersecurity professionals perceive support from their organizations?

This study contributes to the literature of Information System by qualitatively exploring the impact of stress on work among cyber professionals and their perceptions toward organizational support. Our findings emphasize the impact of role ambiguity on job stress and the importance of considering the role of boards along with the use of boards packs to mitigate stress among cybersecurity managers.

2 Background

2.1 The role of cyber-attacks on CISOs job stress and perceived organizational support

Cyber incident is defined by the UK government as a breach in the security policy of a system that impacts its availability, integrity and/or leads to unauthorized or attempted access [13]. The impact of such breaches on the organization are well understood and documented from a reputational, financial or regulatory point of view [14]. The cost of cyber incidents just in the UK is estimated to be £1.4 million with organizations taking 10 months on average to recover [15]. There is also the psychological strain that such cyber incidents impose contributing to the mental health burden of professionals that work in the cybersecurity domain and this is especially true when the incident is caused due to human error [16]. This human error is a direct result of security stress, security fatigue and overstretched cyber practitioners as pointed out by a prior study [17]. When there is a mismatch between the work demands, the knowledge of the individual and the availability of resources, this causes job stress [18]. This can be manifested as alterations to workplace environment and how individuals perceive the situation [19]. It is well documented that cyber practitioners such as the CISOs work in environments that are highly stressful [7]. Indeed, after a cyber incident, they are at a higher risk of exposure to stress-related factors and may perceive varying levels of organizational support. For example, a recent study [20] show that psychological stress is felt by 88% of the CISOs and nearly 90% of them are likely to accept a reduction in their pay. Among CISOs, stress levels is positively correlated with responsibilities that are highly demanding [21]. Additionally, researchers have been exploring how cyber incidents can add psychological pressures on cybersecurity professionals and how they find it difficult to cope with such pressures. In this vein, one research [12] interviewed cyber managers and one of the interviewees responded "this event which lasted the best part of a week was personally very stressful for me, I would go as far as saying this was the most stressful week of my working life" [12]. It is also found that work-related stress and the job responsibility to deal with emerging threats have led to cyber managers being more detached from colleagues [22]. Although there is a negative impact of cyber incidents on how cyber professionals feel towards work, there are factors that can either mitigate or exacerbate how they perceive the support they receive from their organizations. Perceived organizational support is a result of how employees perceive the degree to which they feel their contributions are valued and the extent to which the organization cares about their well-being [9]. Several initiatives can be established by organizations to ensure their cybersecurity professionals feel supported and their work-related stress is lessened. This could encompass provision of further training that enables them to keep abreast of the dynamic threat environment, ensuring communication with boards and budget holders are improved, providing counselling services and better support structures. However, research shows that the individuals experience and perceive similar support levels in a different way [23]. Indeed, determining the extent of assistance required for socio-emotional needs is crucial for cyber practitioners, as it enables them to seek help when necessary [9]. Perceived organizational support initiates a social exchange process in which employees feel motivated to contribute towards the organizational objectives anticipating greater efforts will result in better rewards [24]. The socio-emotional needs such as esteem, approval, emotional support and affiliation are fulfilled by perceived organizational support. As a result, this leads to stronger identification and dedication to the organization as well as enhanced psychological wellbeing [24]. This is hugely relevant specifically for the CISOs as this could have a disproportionate impact when they do not feel supported [25].

2.2 The effects of role ambiguity and board communication

2.2.1 Role ambiguity

Role ambiguity arises when the information provided does not align with the expected behaviour associated with a particular role. In IT work environments, this is a frequently occurring scenario [26]. Among cyber practitioners, researchers [27] show that role ambiguity is a result of misalignment of timelines and goals, lack of clarity on the role and its responsibilities as well as its measurable benefits. This could be due to how the cybersecurity leadership composition is diverse and defining the role to hold individuals accountable is challenging [17]. Therefore, identifying the appropriate skills to support essential skills within the IT department becomes a pivotal moment for a CISO [28]. For example, organizations do not clearly establish expectations for a CISO’s job [29]. Also, studies point out that the CISOs tenure is short and is anywhere around one or two years as a result of higher demands in terms of job responsibilities and lower recovery or personal time [7]. A study showed that 20% of the cyber practitioners will leave an organization due to the role stress they underwent [30]. The perception of support that individuals feel could be affected by role stress that is not manageable as it leads to the work conditions being increasingly stressful. There is a causal relationship between role ambiguity and job stress and one of the antecedents of job stress is role ambiguity [31]. Studies that look at the correlation between perceived organizational support and role ambiguity have found that these factors have a significantly negative correlation [32].

2.2.2 Board engagement in cyber communication

One of the significant factors at the organizational level that could help improving the support needs of the CISOs and mitigate the job stress is their communication with the board of directors. This deals with the engagement of boards on matters concerning cybersecurity. Boards are typically responsible for the organizational corporate governance and therefore have an oversight of the development and implementation of the strategies pertaining to cybersecurity [33]. A key component for ensuring better decision-making process for the boards is a good communication with senior managers [34] such as the CISOs who are tasked with updating the boards regularly. While most other strategic roles follow this practice, this is not very much common when it comes to cybersecurity [25]. Studies have shown that nearly 60% of the CISOs don’t have direct reporting to the boards and even if that happens, they do not see positive results based on the reports submitted. A study by [25] shows that boards do not accept that breaches are inevitable (both in the case of UK and US) as reported by 24% of the 800 board members and CISOs surveyed. The same study also reported that 10% of the CISOs did not know what the boards thought of the breaches. Exploring the factors that drove board engagement in cybersecurity, [33] found that there was an element of communication gap that led to information asymmetry between the boards and the CISOs that caused the boards to disengage. This was in part because the reporting to the boards are technical especially when the boards don’t clearly set out expectations on how the reporting should be done. There needs to be appropriate channels that CISOs can use to communicate cyber challenges effectively to the boards. The communication needs to be done in a timely fashion and the reporting needs to be clearly and concisely documented. Effectively being able to communicate is seen as a means of perceived organizational support by prior research [9]. This shows that tools like the board packs become pivotal for reducing information asymmetries between the boards and the CISOs and hence likely to have a positive impact on perceived organizational support.

3 Research methods

3.1 Data collection and sample

We collected primary data using semi-structured interviews which help to investigate the phenomenon in depth. Due to the challenging nature of quantifying different aspects of individuals' behaviors, qualitative approach becomes crucial in revealing the experiential aspect of individual's lives [34]. For this reason, this approach allows us to collect in-depth, contextual, and genuine narrative concerning participants' everyday experiences on how they feel stress and their perceptions about support from their organizations. This study was approved by the UCL Ethics committee.

We interviewed 24 senior cybersecurity professionals in the UK from varied business sectors. We refer to senior cybersecurity professionals as those who are held accountable by their organization for breaches to their protection and those that are on the (literal) firing line in case of cyber incidents [35]. Five major themes were focused on the interview namely job stress, perception about organizational support, perception about their role, evaluation of the board engagement in cyber communications, and lastly, demographic information about both the individual and the organization. Interviews were conducted between Jan and Mar 21 and on average, took 30 minutes per participant. Participation was voluntary, and all participants provided consent to participate in the research. All interviews were recorded and transcribed by researchers.

Sample. Our paper had a rich sample with 25% participants having the title of CISOs. The remaining participants had job titles including the Head of Information security, Head of technology risk, vice president - cybersecurity, Chief Security Officer, Chief Risk Officer and Information Security Officer. This shows that all participants held senior positions within their organizations. In terms of the tenure, 48% of the interviewees worked between 1 and 3 years in their organization, 24% of them worked between 3 and 5 years in their organization, 16% worked in their organization less than a year and the remaining had worked for over 5 years. It can be said that the tenure for cyber professionals is short with only a marginal group of participants holding their position for up to or more than 5 years. This is depicted in Figure 1. In terms of working hours, 42% of the interviewees worked between 4 and 50 hours, 37.5% of the interviewees worked between 50 and 60 hours a week, and 20.8% worked between 60 and 70 hours a week. The richness of the data collected is also evident in terms of the variation in the industry sector of our participants that bring in diverse perspectives. This is depicted in Table 1.

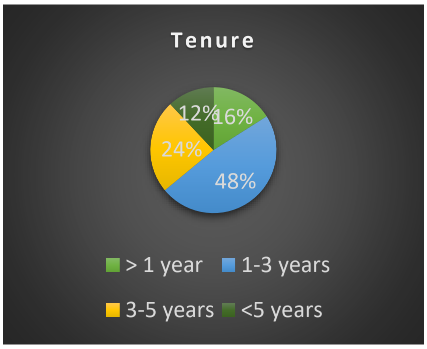

Figure 1: The tenure of CISOs

	Industry
Retail	2
Hospitality	1
Defense	3
Financial Serv.	5
Manufacturing & Engineering	3
Education	1
Mining	1
Marketing	1
Not for profit	1
Media/Technology/Telecom	6
Total organizations	24

Table 1: Sectors represented in the sample.

3.2 Data analysis

We employed a thematic analysis to analyse the interview data and identify emerging themes. This method is widely used in behavioural studies due to its flexibility in revealing patterns in the data [36; 37]. In the phase of data familiarization, we transcribed the raw narrative data and reviewed the transcription to gain a comprehensive understanding of participants' idea and feelings. Subsequently, low -level coding was initiated using Nvivo12, with a focus on addressing our research questions related to conceptualizing, 1) the driving factors that impacts job stress; and 2) the perception about organizational support. The initial step involves the transcription of the interviews, where the analysis starts with reading the narrative data and conducting low-level coding. Initial coded and themes were derived from deductively derived from the theoretical framework. Researchers carefully undertook a review and validation of the coding associated with themes and contributing to researcher triangulation. From the analysis two macro two themes were identified: role ambiguity and board engagement in cyber communication.

4 Results

The themes were presented to all participants that endorsed the elements of the suggested framework and the driving factors around job stress.

4.1 Role ambiguity

The interviews substantiated adverse effects of role ambiguity on job stress. From the interview data, there were different but interconnected dimensions to this that bring together concerns about uncertain expectations, job insecurity, reduced job control and decision-making challenges.

First, having uncertain expectations was a factor and second, the link to mental pressure was raised multiple times. Some participants explained the gap between the outlined job descriptions and the actual expected behavior within their roles. "This is a new dimension of the CISO role – understanding the business objectives and how their work supports that. JDs for CISOs were written by the Big Four and were not challenged. While the qualifications are very technical, the 'C' in the title means the CISO is required to understand the businesses- otherwise they are just a strategic security officer. But this is not often reflected in the job descriptions" [Int09].

One interview also told us the lack of clear guidelines and the persistent experience of ambiguity can lead to mental pressure as CISOs may be unsure about how to meet performance standards and organizational goals: "the job is sold as a CISO but it is technically a "fixit" role. Mental pressures arise because of not being able to do what you were hired to do" [Int17].

This experience goes along with the perception that the role is often a temporary role and leads to reduced job control and decision-making challenges. Indeed, CISOs may face vague or incomplete job descriptions the of the role as not permanent, creating a sense of ambiguity, leaving CISOs uncertain about their long-term contributions, career progression and overall role within the organization. Indeed, one interviewee told us "The CISO turnover is very fast- 2 years in EU and around 18 months in the US. Companies wouldn't invest in their development in the same way they would in longer term team member" [Int10]. On the same line another respondent emphasized that "CISOs are brought in for operational reasons – usually to fix something. They are just seen as a fix for something, maybe regulatory reasons and nothing more." This works as a catalyst when the organization is attacked. A respondent reported: "CISOs are stressed because they are hired as firefighters. The mental pressures that come from "herding cats" to fix things is huge and they are also not given the authority – often due to poor reporting structures" [Int08]. Also, other respondents said ""CISOs are not the budget holders which make it hard to be executive" [Int23]. Furthermore, this perception may heighten stress and frustration when they are unsure about their roles, which ultimately affects their engagement and commitment to the organization "You are excluded from the rest of the organization. Ambiguity in what is being asked of you and what is being provided. That's hard - the C is not real- you're not a chief" [Int24].

4.2 Board engagement in cyber communication and the use of board packs

Organizational support plays a pivotal role in mitigating job stress by proving resources and clear communication. Having a clear communication channel with the Boards as a factor that mitigates their job stress drew a lot of responses – both in agreement and disagreement. The interviews data revealed various dimensions that intertwine different concerns. Some participants explained their feelings of frustration when there is not clear communication and lack of reporting structure. "Frustration of not being able to engage at executive level which makes them want to leave. The organisations that try to cut off the CISO are also the ones that try to bury them deep in organisational reporting structures. While not all CISOs ask for direct reporting to the board, they ask for at least being able to report to someone who is having those high-level conversations. Not being able to do this is a huge stressor" [Int03]. Similarly, the difficulty to communicate with Boards was emphasized from another respondents “Distance from the board puts huge pressure on the CISO’s mental health. There is a lot expected from the CISO who are usually asked to provide metrics (which isn’t usually possible as they are on the defensive side). Also, this is hard as there isn’t enough scope for rigorous or critical exchange” [Int20]. The perception that organizations do not empower CISOs to influence their work environment and the risk of increasing stress level is also reported by another respondents: “CISOs are often asked alienated from the rest of the organisation. They do not have adequate relationships built up the chain and hence become a scapegoat to take the fall when something goes wrong” [Int15]. A respondent highlighted the connection between the lack of organizational support and the absence of adequate corporate governance. “CISOs often hold the risk, it is not passed upwards. Risk should lie with the CEO or the NEDs – the CISOs thus take the shot when there is a breach. This is a failure of corporate governance” [Int11].

Other interviewees strongly disagreed this view and did perceive boards engage in cyber topic: “Interest from the Board and understanding that it is a key risk to the business” [Int08]. Also, participants pointed out the use of boards pack offered as an organizational resource, and hence, support to reduce information asymmetry between cybersecurity professionals and Boards. A respondent commented: “Board templates – board packs- are good when CISOs are required to put in metrics around risk and the risk appetite of the organization. This leads to better board engagement as they are able to decide and determine what they are comfortable with” [Int12]. Similarly, a respondent said: “I think our organization, our board is doing this -board packs- and using all that to support our objective and improve resilience” [Int06]. The use of boards pack is perceived to be effective and clear: “Board templates and board packs are useful as it has metrics that are useful to the board. They also show how these metrics relate to risk. This improves engagement with the board” [Int21]. Other respondents told us that board packs are resources made available from the organization and shared regularly frequently with the boards: “Board packs and templates give you structure. You know you need to fill these in regularly and know what needs to go in there” [Int01]. Similarly, another participant said: “Reports are made to the board each week as needed” [Int10]. This emphasis on boards pack and the links to board engagement can be perceived as a mitigating tool for reducing the level of stress among CISOs. One respondent pointed out: “Board packs help provide insight to boards and not plain data. This helps them to better engage and understand cyber as a business risk, making the CISOs life less taxing” [Int22]. A respondent emphasized: “Because of the board template and its alignment to risk appetite, I have never felt that I have been under pressure to deliver a financial result at the expense of a resilient performance” [Int18].

5 Discussion

Most studies on job stress considered role ambiguity as a driver of job stress [38, 39]. Our results confirm that role ambiguity is linked to the role demands that cybersecurity professionals face in the workplace and their inability to respond to these demands, which leads to stress [40]. Specifically, CISOs reported that unclear job expectations contribute to mental pressure among them. Participants expressed concerns about the discrepancy between job descriptions and actual job responsibilities, particularly the need for CISOs to understand business objectives and support organizations goals. Our interviews enabled us to specify some peculiars points around their job, for instance, a significant finding is the frustration among them regarding their limited authority and lack of control over budget. CISOs often find themselves in firefighting roles, tasked with addressing immediate security concerns without the necessary authority or budgetary control to implement long-term solutions. This is linked to the perception among CISOs that their roles are often viewed as temporary and *fixit* position rather than long-term strategic roles within the organization. This perception leads to reduced job control and decision-making challenges, as CISOs may feel uncertain about their long-term contribution, career progression, and overall role within the organization. The unclarity of the role and the associated stressors also affect CISOs’ engagement and commitment to their organization. Participants reported feelings of exclusion and frustration due to ambiguity in job expectations and limited authority, which undermine their sense of professional identity and diminishes their commitment to their as senior cybersecurity managers.

With respect to the role of organizational support in mitigating job stress among CISOs, our results reported the importance of clear communication channels with boards using board packs. Specifically, they emphasized the impact of distance from the board on CISO's mental pressure, highlighting the pressure associated with the expectation to provide metrics when the organization might not have a clear board pack. This finding is connected to the perception among respondents that organizations do not empower CISOs to influence their work. They reported the failure of corporate governance in this regard, pointing out the need for organizations to allocate resources appropriately and ensure support for CISOs in their roles. However, when the boards do engage in cybersecurity topics the perceived organizational support increases. They reported that boards' interest in cybersecurity is a key risk to the organization. Participants described the use of board packs as an organizational resource to reduce information asymmetry between cybersecurity professionals and boards. The effectiveness of board packs in providing insight to boards and aligning with the risk appetite was highlighted as a mitigating factor for reducing stress among CISOs. Furthermore, the board packs support boards better engage with cybersecurity as a business risk, reducing the burden on CISOs and ensuring a focus on resilient performance rather than solely financial results.

6 Limitations and future research

This study is not free of limitations. First, while we have identified factors that drive stress among cybersecurity managers, such as role ambiguity, we have not evaluated how some specific demographic factors (e.g. age, gender and personality traits) are more influential in changing the perception of stress. Further research can investigate the role of demographic factors in explaining job stress [38]. Second, our study revealed contrasting findings related to the role of boards and the use of template cyber tools as resources given to cybersecurity professionals to mitigate stress. Further research may build on this study to further explore how boards engage in cyber communication and the use of the template as an element of organizational support. Third, our study explores job stress and the perceived organizational support in a context which is idiosyncratic – UK Industrial sectors context. Further research may replicate our study in other contexts to increase the robustness of our results. Finally, in our study we employed a qualitative approach to addressing the research questions. Further research may use a quantitative approach to investigate this phenomenon.

7 Conclusion

Despite the significant influence of job stress on human behavior, there is a lack of comprehensive conceptualization regarding its role within the real cybersecurity context and perceived organizational support among cybersecurity managers. To bridge this gap, we conducted a qualitative study aimed at exploring these phenomena and identifying factors related to role ambiguity and perception of organizational support. Our study shows that CISOs are under mounting pressure, with their jobs on the firing line. Also, our study shows that the pivotal role of organizational support, particularly clear communication with boards using board packs mitigates job stress among CISOs in the cybersecurity domain. Therefore, managing job stress for cybersecurity professionals is hugely important from an organizational perspective as continuity in the job role will ensure better understanding and management of cyber challenges that the organization faces.

Acknowledgements

The authors wish to acknowledge funding received by Lloyd's Register Foundation and the National Cyber Security Centre through the Research Institute for Sociotechnical Cyber Security (RISCS).

References

[1] Paul CL, Dykstra J. Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. Journal of Information Warfare. 2017 Apr 1;16(2):1-1.

[2] National Cyber Security Centre. 2021. Annual Review 2021 - Making the UK the Safest Place to Live and Work Online. ncsc.gov.uk/annual-review-2021.

[3] World Economic Forum. The global risks report 2019 14th edition. Geneva, Switzerland: World Economic Forum.

[4] Lohrmann D. 2020: the year the COVID-19 crisis brought a cyber pandemic. Government Technology. 2020.

[5] Platsis G. The human factor: Cyber security's greatest challenge. InCyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications 2019 (pp. 1-19). IGI Global.

[6] Dykstra J, Paul CL. Cyber Operations Stress Survey ({{{{{{COSS)}}}}}: Studying fatigue, frustration, and cognitive workload in cybersecurity operations. In11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18) 2018.

[7] Nobles C. Stress, burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA–Journal of Business and Public Administration. 2022;13(1):49-72.

[8] Cheng SC, Kao YH. The impact of the COVID-19 pandemic on job satisfaction: A mediated moderation model using job stress and organizational resilience in the hotel industry of Taiwan. Heliyon. 2022 Mar 1;8(3).

[9] Mihalache M, Mihalache OR. How workplace support for the COVID-19 pandemic and personality traits affect changes in employees' affective commitment to the organization and job-related well-being. Human resource management. 2022 May;61(3):295-314.

[10] Shropshire J, Kadlec C. I'm leaving the IT field: The impact of stress, job insecurity, and burnout on IT professionals. International Journal of Information and Communication Technology Research. 2012 Jan;2(1).

[11] Cho J, Yoo J, Lim JI. Analysis of job stress's impact on job performance and turnover of cybersecurity professionals. ICIC Express Letters. 2020;14(4):409-15.

[12] Stacey P, Taylor R, Olowosule O, Spanaki K. Emotional reactions and coping responses of employees to a cyber-attack: A case study. International Journal of Information Management. 2021 Jun 1;58:102298.

[13] National Cyber Security Center.2018. What is a cyber incident. Retrieved 2022 October from https://www.ncsc.gov.uk/information/what-cyber-incident.

[14] Arcuri MC, Brogi M, Gandolfi G. The effect of cyber-attacks on stock returns. Corporate Ownership & Control. 2018;15(2):70-83.

[15] Ashford W. Many UK firms underestimate cost of data breaches, study finds.

[16] Lella I, Theocharidou M, Tsekmezoglou E, Malatras A, editors. ENISA Threat Landscape 2021: April 2020 to Mid-July 2021. ENISA; 2021.

[17] Triplett WJ. Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy. 2022 Jul 22;2(3):573-86.

[18] Dhal HB, Bhatt V, Vora H. Investigating The Mediating Role Of Perceived Culture, Role Ambiguity, And Workload On Workplace Stress With Moderating Role Of Education In A Financial Services Organization. Journal of Positive School Psychology. 2022 Jul 22:9233-46.

[19] Stich JF, Tarafdar M, Stacey P, Cooper C. Appraisal of email use as a source of workplace stress: A person-environment fit approach. Journal of the Association for Information Systems. 2019 Feb 28;20(2):132-60.

[20] Sheridan K. 90% of CISOs would pay for better work-life balance. DarkReading. com.

[21] ISACA. 2020, November 18. Understanding and burning CISO burnout. ISACA.org. Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2020/understanding-and-addressing-ciso-burnout.

[22] Uchendu, B.; Nurse, J.R.; Bada, M.; Furnell, S. Developing a cyber security culture: Current practices and future needs. Journal of Computer Security. 2021, 9, 109.

[23] Yang H, van Rijn MB, Sanders K. Perceived organizational support and knowledge sharing: employees' self-construal matters. The International Journal of Human Resource Management. 2020 Sep 24;31(17):2217-37.

[24] Kurtessis JN, Eisenberger R, Ford MT, Buffardi LC, Stewart KA, Adis CS. Perceived organizational support: A meta-analytic evaluation of organizational support theory. Journal of management. 2017 Jul;43(6):1854-84.

[25] Nominet. 2020. The CISO Stress Report - Life Inside the Perimeter: One Year On. Nominet Cyber Security 8.

[26] Reid M, Allen M, Riemenschneider C, Armstrong D. Affective organizational commitment in state government: the case of IT professionals. American Review of Public Administration. 2008;38(1):41-61.

[27] LeRouge C, Nelson A, Blanton JE. The impact of role stress fit and self-esteem on the job attitudes of IT professionals. Information & Management. 2006 Dec 1;43(8):928-38.

[28] Furnell S. The cybersecurity workforce and skills. Computers & Security. 2021 Jan 1;100:102080.

[29] Hooper V, McKissack J. The emerging role of the CISO. Business Horizons. 2016 Nov 1;59(6):585-91.

[30] Moore JE. An empirical test of the relationship of causal attribution to work exhaustion consequences.

[31] Lambert EG, Hogan NL, Paoline EA, Clarke A. The impact of role stressors on job stress, job satisfaction, and organizational commitment among private prison staff. Security Journal. 2005 Oct 1;18:33-50.

[32] Allen MW, Armstrong DJ, Reid MF, Riemenschneider CK. Factors impacting the perceived organizational support of IT employees. Information & Management. 2008 Dec 1;45(8):556-63.

[33] Gale M, Bongiovanni I, Slapnicar S. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Computers & Security. 2022 Oct 1;121:102840.

[34] Chowdhury NH, Adam MT, Teubner T. Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers & Security. 2020 Oct 1;97:101963.

[35] Kaspersky. 2018. Security Bulletin 2018. Statistics

[36] Braun V, Clarke V. Using thematic analysis in psychology. Qualitative research in psychology. 2006 Jan 1;3(2):77-101.

[37] Piazza A, Vasudevan S, Carr M. Cybersecurity in UK Universities: mapping (or managing) threat intelligence sharing within the higher education sector. Journal of Cybersecurity. 2023 Jan 1;9(1):tyad019.

[38] Tarafdar M, Tu Q, Ragu-Nathan BS, Ragu-Nathan TS. The impact of technostress on role stress and productivity. Journal of management information systems. 2007 Jul 1;24(1):301-28.

[39] Singh T, Johnston AC, D'Arcy J, Harms PD. Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research. Organizational Cybersecurity Journal: Practice, Process and People. 2023 Feb 27.

[40] Hwang I, Cha O. Examining technostress creators and role stress as potential threats to employees'

information security compliance. Computers in Human Behavior. 2018 Apr 1;81:282-93.