Mental health of Cyber Practitioners. A case study on the impact of role ambiguity and boards engagement on job stress and perceived organizational support of CISOs

ABSTRACT

Chief Information Security Officers (CISOs) play a critical role in ensuring business continuity enabling organizations defend against the dynamic threat landscape. As such, the role of the CISO cannot be undermined, and the demands of the role in keeping the organization out of the cyber firing line are quite high. Research on the human stress in cybersecurity is rather limited, as well as the drivers of job stress and perceived organizational support of CISOs. In this research, we look at role ambiguity, and boards engagement in cyber communication as factors that influence job stress and perceived organizational support. By using primary data collected through a survey administered to 24 CISOs from different business sector in UK, we analyze and clarify which factors is the most important drivers for understanding job stress and perceived organizational support. Analytically, we employed an Ordinary last squares (OLS) regression model. Our findings support the role of role ambiguity as opposed to boards engagement in cyber communication in explaining job stress, while role ambiguity and board engagement in cyber communication have a significant effect on perceived organizational support. Understanding these factors can enable organizations to have adequate support mechanisms in place that will ensure their CISOs are energized and ready to take on the cyber challenges thereby maximizing the protection for the organization.

KEYWORDS

Cybersecurity, job stress, perceived organizational support, CISO.

ACM Reference format:

A. Piazza, S. Vasudevan, and M. Carr. 2023. In *Proceedings of ACM SAC Conference, Tallinn, Estonia, Mach 27- April 2, 2023 (SAC'23)*, 8 pages. DOI:

1 INTRODUCTION

In our digital world of ubiquitous connectivity, practices intended to secure information, systems, networks or other valuable assets from unauthorized access, theft, manipulation or otherwise exploitation – i.e. cybersecurity operations - are critical to the safety and business continuity of companies and organizations [1]. From phishing scams, ransomware attacks to targeted hostile acts against critical infrastructure, cyber threats grow year after year [2]. Their notoriety and salience are such that cyber threats have been ranked amongst the leading global risks in the World Economic Forum's 2019 Global Risks Report, only second to global climate change [3]. The COVID-19 pandemic has compounded the severity of cyber threat, increasing the number and sophistication of cyber-attacks during 2021 - a true "Cyber Pandemic" [4]. These trends make visible that 'the single greatest challenge in the cyber domain is also the area most often left unaddressed: the people' [5]. Cybersecurity professionals work in environments that require high vigilance, memory[1] and creative problem-solving [6], skills that are particularly impaired by stress and its negative effects on cognitive abilities, task effectiveness and general well-being. However, whilst stress, fatigue and burnout in cybersecurity operations have been studied to some extent [7], scant attention has been paid in the information system (IS) security literature to the job stress of those in the 'firing line' because of a cybersecurity breach event, who tend to be held liable for the incidents their organizations may suffer: Chief Information Security Officers (CISOs). As CISOs are those who are responsible to respond to a cyber threat in which their response may differ according to the resilience of their organizations, there will be important variation in how CISOs experience their job and the support from their organizations.

Job stress refers to employee's feeling about the work environment [8], while perceived organizational support refers to employee's perception about the extent to which its organization value their contribution and cares about their well-being [9]. When employee's feeling and expectations are not met, the employees may feel stress toward their job and even desire to leave the IT profession altogether [10]. CISOs and other

1 In a cybersecurity task simulation, it was found that the vigilance required for cybersecurity tasks was in line with findings from air traffic control, industrial process control and medical monitoring, fields which demand high levels of attention, memory and visual perception. See Ben D Sawyer and others, 'Cyber Vigilance: Effects of Signal Probability and Event Rate', Proceedings of the human factors and ergonomics society annual meeting (Sage Publications Sage CA: Los Angeles, CA 2014).

cybersecurity leaders are increasingly falling within this pattern [10]. Crucially, certain role-related, organizational and managerial factors – such as role ambiguity (or clarity), and communication dynamics with boards – can be exhausting, taxing and stressful, yet can be readily turned into *positive* stressors if acted upon, thereby allowing CISOs to attain a better work-life balance, experience less overall negative stress, and generally be able to enjoy a more fulfilling work environment. To this end, the question asked in this study is which of the factors drive job stress and perceived organizational support of CISOs? So far, we know very little about how organizations can assist cyber employees toward their work. Also, most studies in IS security focus on the technical angle of dealing with cyberthreat and despite the significant role that human actors play in the design and execution of cybersecurity operations, studies on human stress in cybersecurity efforts remain a rather under-researched topic [11-12]. The aim of this study is to investigate the relationship between job stress, perceived organizational support and role ambiguity and boards engagement in cyber communication. The opportunity to address the above question is provided by primary data collected through a questionnaire-based survey administered to 24 CISOs from different business sectors in UK. This study contributes to the literature of IS in understanding how organizations can encourage their employees' job to reevaluate the factors that are likely to have a significant impact on the robustness and resiliency of their cybersecurity programmes.

2 Background

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

The UK government defines a cyber incident as "a breach of a system's security policy in order to affect its integrity or availability and/or unauthorized access or attempted access to a system or systems" [13]. The financial, reputational, and legal damage that cyber incidents cause to an organization are well documented and widely understood [14]. For instance, [15] has shown that the cost of cyber incidents in the UK is 1.4£ million with a recovery time of 10 months. However, cyber incidents also impose a level of psychological strain and mental health burden for senior managers working in cybersecurity. This is particularly so when cyber incident is thought to be the result of human error [16]. Previous study has suggested that human error is caused by security fatigue and stress and the overextension of cyber practitioners [17]. Job stress is defined as a mismatch between individuals' knowledge, resources available and the work demands [18]. This can take the form of shifts in the working environment and the perceptions of that situation [19]. Research has shown that cyber practitioners like CISOs work under highly stressful environment [7]. Indeed, CISOs are more likely to be exposed to various risk factors concerning their level of stress and their perception of organizational support following a cyber incident at work. For instance, [20] suggests that 88% of CISOs feel psychological stress and 90% of them are likely to take a pay cut. [21] reports a positive correlation between the high demanding responsibilities and the high level of stress among CISOs. [12] have explored the psychological pressure that cyber incidents can have on cybersecurity managers and the difficulty they experience in trying to cope with this. One of cyber managers they interviewed told them that "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]. Furthermore, researchers have emphasized that cyber managers are more likely to be detached with their colleagues because of the work-related stress and the responsibility of dealing with an emerging threat [22].

While a cyber incident can negatively affect the way that cybersecurity managers feel towards their work, this can be generally mitigated or exacerbated by the extent to which they receive (or perceive) support from their organizations. Perceived organizational support occurs when employees develop a general perception about the extent to which their organization values their contributions and cares about their well-being [9]. Organizations can establish multiple initiatives to support their cybersecurity managers to lessen their work-related stress. This may take different forms, including additional training to stay abreast of threats, improvements in communications to the boards and budget holders, counselling, support structures, offering flexible schedules to strike an adequate work-life balance, and even softer forms of organizational support, such as acknowledging the difficulties employees suffer as a result of a given event (such as a security breach), and showing appreciation of the efforts employees make. Research suggests that individuals perceive and experience the same level of support in a different manner [23]. Indeed, ascertaining the level of support with socio-emotional needs is important for cyber practitioners as they can request it when needed [9]. Perceived organizational support triggers a social exchange process whereby employees feel compelled to help the organization achieve its goals and expect that stronger efforts on their part will lead to greater rewards [24]. Importantly, perceived organizational support fulfils socio-emotional needs (approval, esteem, affiliation, and emotional support), resulting in greater identification with, and commitment to, the organization, as well as greater psychological well-being [24]. This is extremely relevant for CISOs when they feel unsupported, and these initiatives may have a disproportionate impact [25].

We considered the potential antecedents of perceived organizational support and job stress to be role ambiguity and organizational action like board engagement in cyber communications.

2.2 The effects of role ambiguity and Board communication

2.2.1 Role ambiguity. Role ambiguity occurs when the information does not match with the behavior expected in a role. This is commonly the scenario in IT work environments [26]. [27] show that the lack of unclear direction related to the roles and responsibilities; lack of measurable benefits; and difference in goals and times are the sources of role ambiguity among cyber practitioners. The reason behind that is because cybersecurity leadership include different people, and this creates difficult to define leadership roles and distinguish leaders accountable [17]. Therefore, the identification of the right skills to support the

required roles and responsibilities in IT department is a turning point for a CISO [28]. For instance, [29] found that organizations do not usually set up a clear expectation of the job the CISO is expected to perform. Other study points out that the tenure of CISO tends to range from one to two years as a result of the increase of the demand responsibilities, the decrease of personal and recovery time [7]. [30] found that 20% of cyber practitioners are more likely to quit their organizations because they experience high role stress. The unmanageable role stress situation can make the work condition stressful and different in the perception of the support. Findings about the role ambiguity in the job stress relationship have reported a causal relationship in which role ambiguity is an antecedent of job stress [31]. While findings about the role ambiguity in the perceived organizational support have reported a significant negative correlation between perceived organizational support and role ambiguity [32].

2.2.2 Board engagement in cyber communication. At organizational level, an important factor that may address CISOs support needs and influence job stress is the communication between CISOs and Boards of Directors (BoDs). This can refer to how boards engage with cybersecurity. Boards of Directors (BoDs) are responsible for the corporate governance of the organization, including the development and the implementation of the cybersecurity strategy [33]. A key element in general, for the decision-making process of boards is the communication with the senior managers [34] (e.g. CISOs), whereby the senior managers (e.g. CISOs) regularly update them. While this is common in other strategic roles, this is not the case in cybersecurity [25]. Research suggests that 60% of surveyed cyber practitioners do not report cyber-incidents to their BoDs and when that happens, they tend to admit negative results from reports. A survey by [25] with 800 BoDs and CISOs in the US and the UK reports that, 24% of CISOs said that their boards did not accept that breaches are inevitable; this was confirmed by 24% of BoDs, who indicated that they in fact do not consider breaches as inevitable, and a further 10% admitted that they did not know it. [33] that have explored the factors that drive boards engagement in cyber topic, found that information asymmetry is an element of the communication gap between board members and CISOs, leading to the directors' disengagement from technical reporting where the expectations on reporting activities from boards are not set. As such, board-CISO communication can be facilitated when the communication channel used help CISOs to clearly outline cyber challenges to the boards, whereby the communication occurs in a timely manner through well-documented processes. Studies have shown that the ability to effectively communicate can also be perceived as organizational support [9]. Tools such as board packs, thus become crucial for CISOs to reduce information asymmetries and to ensure that they are able to handle cyber challenges in an efficient manner, which in turn has a positive impact on them.

3 RESEARCH METHODS

3.1 Data collection and sample

We collected primary data using an online questionnaire through the Opinio platform. Opnio platform has used in different studies [35-36-37] as it has the advantage of reducing the time to collect data. The questionnaire was administered to 24 senior cybersecurity managers from different business sectors in UK. We refer to senior cybersecurity managers as those in the (literal) firing line in the event of a cyber events and those generally held accountable for any cybersecurity incidents their organization may suffer [38]. A pilot questionnaire was administered to 10 senior cybersecurity managers. All of them provided valuable feedback in designing the final version of the questionnaire. The questionnaire focused on five main themes: 1) job stress; 2) perception about organizational support; 3) perception about their role; 4) evaluation of the board engagement in cyber communications;5) and finally, demographic information at individual and organizational levels. Data collection took place between January and March 2021. A page explained that participation was voluntary, and the data would be kept in strict confidence and in line with the data protection act. The ethics form for data collection was approved from the UCL ethics committee.

Sample. The richness of our sample is based on the fact that 25% participants were CISOs and the other were Vice- President of Cybersecurity; Head of Information Security; Head of Technology Risk; Chief Risk Officer; Chief Security Officer; ISO. This indicates that they occupied a senior manager role within the organization. Fig. 1 shows that 48% of the respondents had worked at their organization between 1-3 years, 24% of respondents had worked at their organization between 3 to 5 years, and the remaining had worked less of one year (16%) and more than 5 years (5%). This shows that their position lasts only for short-term period when only a marginal percentage of senior managers hold their position up to 5 years, while most of them cannot take their job for more than 3 years. Regarding the working hours a week, 42% of the respondents worked between 40 to 50 hours a week, while 37.5% of respondents worked between 50 to 60 hours a week, and 20.8% worked between 60 to 70 hours a week. Furthermore, a sector analysis of our sample reports a significant variation which contributes to the richness of our collected data (Table 1).

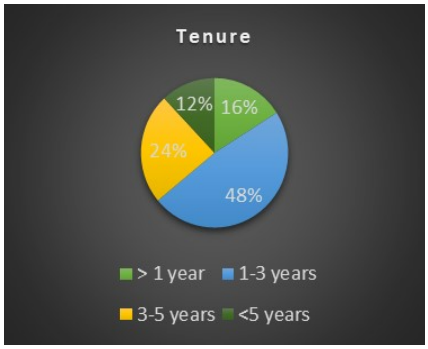

Figure 1: The tenure of CISOs

	Industry
Retail	2
Hospitality	1
Defence	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 Variables and measures

There are four variables[2] used in this study namely: *job stress*, *perceived organizational support*, *role ambiguity* and *board engagement in cyber communication*. For all the variables, a 5-point Likert scale ranging from 1 to 5 was used with 1 strongly disagree to 5 being always agree. For each of the variables, 3/4 items were used (see table 2). A Cronbach Alpha test was performed for internal validation – a value of 0.70 or more indicates a good internal consistency [39] (see table 2).

Three demographic variables were selected as controls, namely job title (i.e., categorical variable representing the different positions that the participant occupies); tenure at the current organisation (i.e., number of months worked at the current organisation); and weekly workhours (i.e. number of hours worked at the current organisation).

Variable	Item-included	Cronbach Alpha
Job stress[3] (JS)	I feel nervous because of my job	0.80
	In the event of a significant cyber incident, I am on the firing line which increases my level of stress	
	My work-related stress impacts my performance in a negative manner	
	My organisation's risk appetite is a hinderance to brining creative/innovative ideas	
Perceived organisational support[4] (POS)	I feel I have the necessary training and support from my organization to carry out my role effectively	0.78
	There are support structures in the organization to help with work-related stress	
	The organization cares about my well-being	
Role ambiguity [5] (RA)	I feel I understand the business objectives and how my work supports these	0.75
	Lack of clarity of job description and responsibilities	
	I feel I have all the skills I need to speak the language of the board	
	Feeling that the information that you have presented is being edited by others before it is passed on to the boards	
Boards engagement in cyber communication (BECC)	How frequently do you use templates for board papers	0.73
	How frequently was information about templates shared with you in a timely manner	
	Feeling that these templates are useful	
	Feeling that these templates facilitate clear communication with boards	

Table 2: Variable and measurement items.

[2] We also performed a factor analysis (FA) to investigate the underlying dimension that explain the relationship between the multiple items. This is a well-known method used in different fields, for more information please refer to Nunnally J, Bernstein I. Psychometric theory. New York: McGraw-Hill, 1994. The results for the FA are available upon request.

[3] The measure was based on a scale inspired by Cheng, S. C., & Kao, Y. H. (2022). 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, 8(3), e09134. However, we modified and added a new item to better specific aspect of job stress among CISOs

[4] The measure was based on a scale inspired by Eisenberger et al. (1986). Perceived organizational support. Journal of Applied psychology, 71(3), 500. However, we modified and added a new item to better specific aspect of support for CISOs

[5] The measure was based on a scale inspired by Mohtman A et al. (1978). Participation in decision making: a multidimensional perspective. Educ. Admin. Q.14:13-29. However, we modified and added a new item to better specific aspect of role ambiguity for CISOs

4 RESULTS AND DISCUSSION

Pearson's correlation coefficients were calculated, and the results reported in table 3. Work hours had a statistically significant and positive association with job stress: as workhours increased, so did job stress. Work hours was the only demographic variable that had significant correlation with job stress. While most senior leadership members on average work longer hours, studies [25] show there is a spike in working hours especially during stressful times such as cyber incidents. Role ambiguity had statistically negative association with job stress: as the role ambiguity increased the job stress decreased; similarly perceived organizational support had statistically negative association with job stress: as perceived organizational support increased the job stress decreased. Role ambiguity had a statistically significant positive association with perceived organizational support: as role clarity increased, so did perceived organizational support. Board engagement in cyber security had a statistically significant positive association with perceived organizational support: as board engagement in cyber security increased, so did perceived organizational support.

Variables	1	2	3	4	5	6	7
1.JS	1.000						
2.POS	-0.596*	1.000					
3.RA	-0.672*	0.645*	1.000				
4.BECC	-0.221	0.565*	0.265	1.000			
5.Job title	0.200	-0.1173	-0.161	0.257	1.000		
6.Tenure	0.302	-0.0522	-0.342	-0.017	-0.025	1.000	
7.Workhours	0.405*	-0.091	-0.334	0.113	0.264	0.215	1.000

Table 3: Pearson's correlation coefficient among the variables. Note:* p < 0.05; ** p < 0.01; *** p < 0.001

The ordinary least squares (OLS) regression results with job stress and perceived organizational support as the dependent variables are presented in tables 4-5 respectively. In examining the OLS regression results for job stress as the dependent variable, only the parameter associated with role ambiguity had a significant and negative impact on job stress. This suggests that CISOs who have a clear understanding of their role are less stressed. None of the control variables had a significant impact on the job stress, nor did board engagement in cyber communication.

Intercept	4.0650**(1.369) [1.2141]
RA	-0.7312*(.2744) [-1.3078]
BECC	-0.0953 (.1373) [-.3837]
Job title	.0183 (.0341) [-.0533]
Tenure	.0012(.0029) [-.0048]
Work hours	.0205 (1.3569) [1.2141]
Observation	24
R^2	0.5083

Table 4: Results for job stress. Note: Robust standard errors are given in parentheses; 95% confidence intervals are given in brackets; Significance levels: ***p ≤ 0.001; **p ≤ 0.01; *p ≤ 0.05; †p ≤ 0.1.

For the perceived organizational support OLS equation, the results change: role ambiguity and board engagement in cyber communication had a statistically positive impact on the perceived organizational support.This suggests that an increase of each independent variables is associated with an increase of the dependent variable. In other words, i) when CISOs have a less understanding of their role (higher level of role ambiguity) they receive higher support from the organizations; 2) when Boards show higher engagement in the communication, CISOs perceive high support from the organizations. Regarding the control variables, all the control variables had no statistically impact on the dependent variable as shown in table 5.

Intercept	-4987(1.3329) [-3.2990]
RA	0.8812*(.2696) [.3147]
BECC	0.3776*(.1348) [.0942]
Job title	-0.0326(0.3350) [-.1030]
Tenure	0.0024(.0028) [-.0035]
Work hours	0.0067 (.0184) [-.0321]
Observation	24
R^2	0.5209

Table 5: Results for job stress. Note: Robust standard errors are given in parentheses; 95% confidence intervals are given in brackets; Significance levels: ***p ≤ 0.001; **p ≤ 0.01; *p ≤ 0.05; †p ≤ 0.1.

5 CONCLUSION

We looked at the factors that has an impact on the job stress of CISOs and showed that clarity in the role, improved

perception of organizational support and better engagement of the boards with cybersecurity will have a positive impact on reducing job stress of CISOs. Managing job stress for CISOs 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 face. It is imperative that oranizations are able to not only find the right talent for the job but also retain such talent – our study shows that CISOs are under a mounting pressure with their jobs on the firing line. What is worrying is that while issues of mental wellbeing and stress are studied at organizations, not much of this has transpired into action, especially at senior leadership levels. Higher stress levels will ultimately lead to a burnout crisis, hampering the CISOs to be effective in their role. A CISO who is less stressed and more empowered is able to better deal with the cyber challenges and the organization is thus better protected.

ACKNOWLEDGMENTS

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] CL Paul and J Dykstra. 2017. *Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations*. Journal of Information Warfare 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. 2019. *The Global Risks Report 2019 14th edition*. Geneva, Switzerland: World Economic Forum.

[4] D. Lohrmann. 2020. *2020: The year the COVID-19 Crisis Brought a Cyber Pandemic*.(GovTech,11 December 2020). https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

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

[6] Dykstra, J., & 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 (CSET 18).

[7] Nobles, C. 2022. *Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem.* HOLISTICA–Journal of Business and Public Administration*,* 13*(1), 49-72.*

[8] Cheng, S. C., & Kao, Y. H. 2022. *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*,* 8(3), e09134.

[9] Mihalache, M., & Mihalache, O. R. 2022. *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, 61(3), 295-314.

[10] Shropshire, J., & Kadlec, C. 2012. *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, 2(1).

[11] Cho, J., Yoo, J., & Lim, J. I. 2020. *Analysis of job stress's impact on job performance and turnover of cybersecurity professionals.* ICIC Express Letters, 14(4), 409-415.

[12] Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. 2021. *Emotional reactions and coping responses of employees to a cyber-attack: A case study*. International Journal of Information Management, 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, M. C., Brogi, M., & Gandolfi, G. 2018. *The effect of cyber-attacks on stock returns*. Corporate Ownership & Control, 15(2), 70-83.

[15] Ashford, W. 2012. *Many UK firms underestimate cost of data breaches, study finds.* Retrieved 2022 October from https://www.computerweekly.com/news/2240171040/Many-UK-firms-underestimate-cost-of-data-breaches-study-finds.

[16] Enisa. 2021. *Threat Landscape 2021*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[17] Triplett, W. J. (2022). *Addressing Human Factors in Cybersecurity Leadership*. Journal of Cybersecurity and Privacy, 2(3), 573-586.

[18] Dhal, H. B., Bhatt, V., & Vora, H. (2022). *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, 9233-9246.

[19] J.F. Stich, M. Tarafdar, P. Stacey, S.C. Cooper. 2019. *Appraisal of email use a source of workplace stress: A person-environment fit approach*. Journal of the Association for Information Systems, 20 (2), p.2.

[20] Sheridan, K. 2020, June 6. *90% of CISOs would pay for better work-life balance.* DarkReading.com. Retrieved from https://www.darkreading.com/risk/90--of-cisos-would-cut-pay-for-better-work-life-balance/d/d-id/1336995.

[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, M. B., & Sanders, K. 2020. *Perceived organizational support and knowledge sharing: Employees' self-construal matters*. The International Journal of Human Resource Management, 31(17), 2217–2237.

[24] J Kurtessis, J. N., Eisenberger, R., Ford, M. T., Buffardi, L. C., Stewart, K. A., & Adis, C. S. 2017. *Perceived organizational support: A meta-analytic evaluation of organizational support theory*. Journal of management, 43(6), 1854-1884.

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

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

[27] LeRouge, C., Nelson, A., & Blanton, J. E. 2006. *The impact of role stress fit and self-esteem on the job attitudes of IT professionals*. Information & Management, 43(8), 928-938.

[28] Furnell, S. 2021. *The cybersecurity workforce and skills*. Journal of Computers & Security, 100, 102080.

[29] Hooper, V., & McKissack, J. 2016. *The emerging role of the CISO*. Business Horizons, 59(6), 585-591.

[30] J.E. Moore. 1998. *An empirical test of the relationship of causal attribution to work exhaustion consequences*, in: M.A. Rahim, R.T. Golembiewski (Eds.), Current Topics in Management, JAI Press, Inc., Stamford, CT, 1998, pp. 49–67.

[31] Lambert, E. G., Hogan, N. L., Paoline, E. A., & Clarke, A. 2005. *The impact of role stressors on job stress, job satisfaction, and organizational commitment among private prison staff*. Security Journal, 18(4), 33-50.

[32] Allen, M. W., Armstrong, D. J., Reid, M. F., & Riemenschneider, C. K. 2008. *Factors impacting the perceived organizational support of IT employees*. Information & Management, 45(8), 556-563.

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

[34] Landefeld, S. M., Mejia, L. R., & Handy, A. C. 2015. *Board tools for oversight of cybersecurity risk*. The Corporate Governance Advisor, 23(3), 1-9.

[35] Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J., & Carr, M. 2018. *Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?. In Living in the Internet of Things:* Cybersecurity of the IoT-2018 (pp. 1-9).

[36] Riel, D. 2020. *Faster Acquisition: Putting the Priority on Speed*.

[37] Jones, J. H., & Salathé, M. 2009. Early assessment of anxiety and behavioral response to novel swine-origin influenza A (H1N1). PLoS one, 4(12), e8032.)

[38] Kaspersky. 2018. *Security Bulletin 2018*. Statistics

[39] Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. 2010. *Multivariate Data Analysis, 7th ed*., MacMillan Publishing Company, New York, NY.