Impact of Technical Controls, Accountability, and Monitoring on the Job Performance of Employees: Assessing the Mediating Role of Stress

Mohammed Alqahtani
University of Technology Sydney, Mohammed.Alqahtani@student.uts.edu.au

Eila Erfani
University of Technology Sydney, eila.erfani@uts.edu.au

Impact of Technical Controls, Accountability, and Monitoring on the Job Performance of Employees: Assessing the Mediating Role of Stress

Full research paper

Mohammed Alqahtani
School of Information, Systems and Modelling
University of Technology Sydney
Sydney, Australia
Email: Mohammed.Alqahtani@student.uts.edu.au

Eila Erfani
School of Information, Systems and Modelling
University of Technology Sydney
Sydney, Australia
Email: Eila.Erfani@uts.edu.au

Abstract

One of the major cyber security challenges that organisations face is understanding the contribution of internal organisational, personal, and technical factors. Cybercriminals are widely discussed in mainstream media with respect to data breaches and attacks, but most security breaches are caused by employees, whether intentionally or unintentionally, due to non-compliance with cyber security measures. In the interests of cyber security compliance, organisations implement measures such as technical controls, accountability procedures and monitoring. Some organisations compel employees to comply with these and other cyber security policies and procedures, which may increase compliance but induce stress and reduce employees' performance.

The current research sought to determine the relationship between technical cyber security controls, accountability, monitoring and the job performance of the employees, as well as the mediating role of stress. Data was collected between March to June 2021 from 302 participants (211 men, 91 women and all adults) working in Saudi Arabian organisations. The data was analysed using mediation analysis in SPSS. The results indicate a significant positive relationship between the use of technical controls, accountability procedures and monitoring for cyber security purposes and employee stress, and a significant direct negative relationship between stress and job performance. These results are novel and directly applicable in organisational settings in which cyber security is an important objective. It would also be helpful to tell employers what they can do to improve cyber security without increasing stress.

Keywords Technical Controls, Accountability, Monitoring, Cyber Security, Stress, Job Performance.

1   Introduction

Digital technology has experienced unprecedented development and growth over the past few decades, and contributes substantially to innovation, productivity, and economic growth. However, the widespread use of digital technology means organisations are vulnerable to cyberattacks, denial of service, data breaches and other cyber security issues (Cukier, 2016; Ponemon, 2019). Recently, a survey reported that an average of 2244 cyberattacks occurs per day worldwide (Cukier, 2016). Cyberattacks can cause substantial financial losses: a 2019 study estimated the global annual cost of data breaches as $3.92 billion, a 1.5% increase from the preceding year (Ponemon, 2019). Another study found that 4.1 billion data records were exposed during the first half of 2019 (Risk Based Security, 2019).

In response to increased incidence of cyberattacks and data breaches, organisations have introduced various information security controls and measures. These measures mainly consist of technical cyber security controls, accountability procedures and monitoring, designed to help and sometimes compel employees to comply with cyber security policies and procedures (Donalds & Osei-Bryson, 2020). These measures may impose a heavy burden on employees in the form of stress that can lead to low job performance (Ament & Haag, 2016; Cram et al., 2021; D'Arcy et al., 2014; Park & Cho, 2016).

Lee et al. (2016) conducted a survey to identify the role of stress in information security compliance activities (ISCAs). They found that 63.6% of surveyed employees had experienced stress due to ISCAs, and 42.7% had suffered difficulties in carrying out their actual work due to ISCAs. Other research contended that imposition of security controls places stress on employees, which (ironically) reduces their security compliance (Alqahtani & Erfani, 2021; Bulgurcu et al., 2010). Moreover, increased security requirements and information security stress make employees more likely to violate information security procedures (D'Arcy et al., 2014; D'Arcy & Greene, 2014). Research has also identified that stress lowers employees' job satisfaction and morale, thereby harming personal productivity and organisational performance (Ragu-Nathan et al., 2008). Understanding how enforced cyber security compliance causes stress for employees and the effect of stress on security compliance is an important topic for information systems research.

There is little published empirical evidence about employees' stress and its relationship to technical controls, accountability, monitoring and job performance. Hence, this study was designed to investigate these issues. It aimed to identify the mediating role of employees' stress in the relationship between technical controls, accountability, monitoring and job performance. The results indicate that stress caused by information security compliance activities is directly reducing employees' performance.

The rest of this article is organised as follows. Variables of interest are discussed in section 1.1 and hypotheses are developed, and the results of a detailed literature review in section 2. Section 3 depicts the theoretical model. In section 4, methods of data collection and analysis are presented; the results are presented in section 5 and discussed in section 6. Finally, the study's conclusions are presented in section 7.

2   Variables of Interest

The following measures are implemented frequently in organisations to enhance and sometimes enforce compliance with cyber security policies and procedures.

2.1.1   Accountability

Accountability – defined as "all employees are responsible for their actions, behaviours, performance and decisions" (Amin, 2019) – is considered a key factor in information security and compliance with security policies and procedures (CommandHound, 2019; Vance et al., 2013). In any organisation, some employees complete their assigned tasks efficiently and as required, while others perform less well (Chen et al., 2012; CommandHound, 2019; Liu et al., 2021). Hence, some organisations offer incentives to motivate employee performance; however, some employees remain unmotivated. Thoms et al., 2002) identified a positive relationship between accountability and employee performance; other researchers confirm that accountability generates better results than rewards or incentives (Chen et al., 2012; CommandHound, 2019; Feigenbaum et al., 2011; Liu et al., 2021; Vance et al., 2013).

The theory behind the relative effectiveness of a culture of accountability is that when employees are directly responsible for a said task or for following policies or procedures, there is a higher rate of task completion (Chen et al., 2012). If an employee knows that their performance is monitored and that they will be accountable for their actions related to cyber security, they will be more cautious and strive to comply with security policies while completing their tasks efficiently (Feigenbaum et al., 2011). (Note

that technical controls and accountability are best applied simultaneously, because if employees fail to be accountable, technical controls will force them to use the correct procedure (Vance et al., 2012, 2013).)

There are some limitations to accountability, notably that enforced accountability may cause employees undue and counterproductive stress. To test this possibility, the current study formed the following hypothesis.

H1: Accountability is a significant predictor of stress among employees implying that increased perception of accountability may decrease performance of the employees.

2.1.2 Monitoring

Monitoring is directly related to accountability, because without monitoring, accountability is impossible. If individuals' perception of accountability is strong and they are aware that monitoring is ongoing, their compliance behaviour will be stronger. Hence, monitoring is often used to facilitate security compliance.

Employees are one of the major sources of cyber security problems (Harris & Martin, 2019; Liu et al., 2021; S. Raschid Muller & Mary L. Lind, 2020). This may take the form of errors, as well as intentional or unintentional supply of data to criminals. Many organisations now use employee monitoring software, physical surveillance, electronic communication surveillance, internet activity monitoring and desktop monitoring to prevent these issues from occurring (Majumdar, 2020). Such monitoring may be beneficial for the organisation's cyber security but may be frustrating and even harmful for employees. Indeed, research has found that electronic monitoring causes stress and other psychological issues among employees (Alder, 2001). To investigate this relationship in the current study, the following hypothesis was developed.

H2: Monitoring coupled with accountability has a significant relationship with stress implying that if monitoring increases employee's stress also increases which may ultimately effect job performance of the employees.

2.1.3 Technical Cyber security Controls

Technical controls (also called logical controls) are deployed to protect an organisation's digital infrastructure and data from breaches and information leakages. Controls are meant to provide automatic protection against unauthorised access or misuse of information, support the application of data security requirements, and facilitate quick detection of security breaches (Dempsey et al., 2011; Toth et al., 2014). Examples of technical controls include data loss prevention solutions, authentication solutions, two-factor verification, biometric authentication, access control lists, encryption, anti-malware, intrusion detection and prevention systems and constrained interfaces.

Technical measures help – and sometimes force – employees to comply with cyber security policies and procedures and to maintain the confidentiality, integrity and availability of critical data (Dempsey et al., 2011). Although technical measures can be effective, forcing employees or end-users to follow specific steps may irritate or frustrate them and sometimes even weaken their intention to maintain security compliance (Toth et al., 2014). Hence, these controls may cause stress among employees who do not follow them willingly. Hence, the following hypothesis was formulated for testing in the current study.

H3: Enforced technical security controls cause stress that leads to low work performance.

2.1.4 Psychological stress

Hans Selye introduced the concept of psychological stress in 1930, defining it as "a mental and physical movement and the reaction of an individual in order to provide necessary adaptation against any physical and psychological stimulants" (Viner, 1999). More recently, Christina et al. (1996) explained the phenomenon of stress as "a mediating and threatening part of a complex and dynamic interaction system between the individual and the individual's environment", and Roberts (2003) stated that stress is "a concept that affects individuals and their behaviour, work efficiency, and the relationships with other people". Although it can lead to tension and depression (Langford et al., 2020), stress is not a solely negative concept; it can motivate people to seek, work, create new things, and solve problems (Polat, 2008). Some employees respond to positive stress by improving their performance and compliance, while others respond negatively to the stress caused by accountability, monitoring and enforcement of technical controls. To learn more about the effect of stress, the current study tested the following hypotheses.

H4: Stress has a significant impact on employees' job performance

H5: There is an indirect relationship between accountability, monitoring, technical controls, and job performance implying that's stress plays a mediating role among this relationship.

3   Literature Review and Theoretical Background

This section explores the literature on the variables of interest: cyber security technical controls, accountability, monitoring, stress, and job performance of the employees.

Stress is defined herein as stimulating events (such as accountability, monitoring and technical controls) which cause negative reactions (such as loss of interest in work, inattention and low morale) among people who encounter them (Lambert & Lazarus, 1970). Ragu-Nathan et al. (2008) developed the concept of technostress, relating it to five aspects of organisational IT usage: overload, invasion, complexity, insecurity, and uncertainty. This construct specifically refers to employees' struggle to deal with constantly evolving workplace technologies and the social and cognitive demands related to their use (Rodell & Judge, 2009). In addition, D'Arcy et al. (2014) coined the term security-related stress (SRS) to describe the stress and fatigue resulting from the security requirements and demands that organisations impose on employees. They argued that SRS is a form of psychological stress that can be caused by external as well as internal security-related requirements.

Several theories of work-related psychological distress have been developed. The person–environment fit theory holds that work-related stress is caused by the lack of fit between the individual's skills, abilities, resources, and the demands of the work environment (Caplan, 1987). The lack of fit may be a subjective perception or an objective reality (French et al., 1974). Another theory of work stress is job demand control theory, which holds that work-related stress can occur due to conflict between confusing and/or enforced demands that may include cognitive or emotional demands, as well as interpersonal conflicts and workload (Van Der Doef & Maes, 1999). Bheer et al. (2001) claimed that employees who experience conflict between high demands and have low control over their job and related decisions are at high risk of psychological distress.

Employees vary considerably in their compliance behaviour and responses to workplace demands. Some employees will comply with security policies and guideline irrespective of personal or organisational factors, while others may violate policies due to their inability to overcome the same factors (Cram et al., 2021). Given such variability among employees, organisations have little choice but to enforce accountability and monitoring in an attempt to maximise cyber security compliance (Furnell & Thomson, 2009). However, enforcement may cause stress. Siegel-Jacobs and Yates (1996) claimed that accountability can increase decision stress among employees, and earlier research linked accountability with stress, stereotyping and reduced cognitive complexity of employees (Gordon et al., 1989). Increased accountability and related stress can result in wasted resources, reduced compliance behaviour and ultimately low work performance (Adelberg & Batson, 1978).

Research shows that monitoring affects the performance and stress levels of employees. Although workplace monitoring can be represented as a necessity and the right of the employer (Kiziloglu, 2018), it can reduce worker's morale, motivation and performance by increasing stress (D'urso, 2006). Aiello and Kolb (1995) observed skilled and unskilled people entering data with and without monitoring in a laboratory setting. They found that even highly skilled people made more mistakes under monitoring than their non-monitored counterparts. Kiziloglu (2018) surveyed 218 employees, from low-skilled workers to top-level managers, and found that they perceived monitoring as a negative factor linked strongly to workplace stress.

Technical controls can not only cause stress but high turnover among employees. Hassan (2014) collected data from 103 employees of IT companies that had implemented technical measures. He sought to identify the effect of organisational commitment, job stress, job characteristics, promotion opportunities, pay level and rewards, quality of work life and job satisfaction on job turnover. Hassan (2014) found that job stress was the most powerful factor affecting turnover among employees in environments in which technical controls were enforced.

Some researchers have studied the effects of stress on the job performance of employees who are accountable and monitored for their compliance with technical controls. Jamal (1984) studied 440 hospital workers in Canada, and found a strong negative relationship between job stress and job performance, a finding confirmed by Affleck (1999). Similarly, Jamal (2007) found a significant and negative linear relationship between job performance and stress among the employees of a US-based multinational company, and AbuAlRub (2004) determined that the job stress and job performance of 263 American hospital nurses were highly correlated.

Most of the cited research is a bit old and lacks the current research on employee accountability and its potential relationship with stress. Also, solid evidence (Ryan et al., 2017) motivates us to study the mediating relationship of stress due to technical controls, accountability, and monitoring of employees' job performance. Therefore, the current study aims to provide updated evidence of the role of technical controls, accountability, and monitoring on employees' job performance due to stress.

4   Theoretical Model

The literature provides some indirect evidence that technical cyber security controls, accountability and monitoring can lead to stress in employees, and that stress decreases employee performance. Based on these findings, theoretical model for the current research was developed a (Fig. 1).
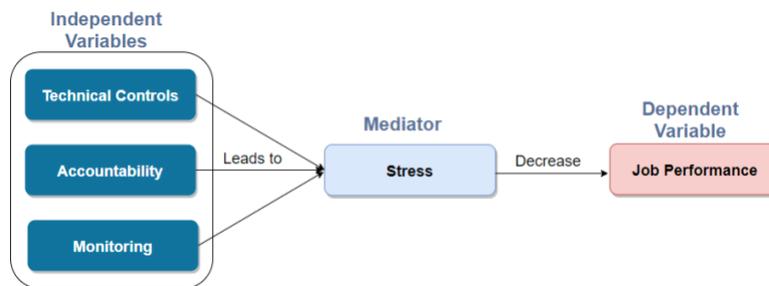
Figure 1 - Theoretical Model

5   Research Methodology

The current study employed a correlational research design. Its aim was to identify the impact of the independent variables (accountability, monitoring and technical controls) on the dependent variable (job performance) in the presence of a mediating variable (stress).

Data was collected between March to June 2021 using an online Google Forms questionnaire that was designed based on previous theoretical basis and constructs. Potential respondents were approached individually, and these willing to participate were sent an online link to the questionnaire via WhatsApp, email, Facebook, or LinkedIn. Snowball sampling was used for sampling. As per our request, the initial respondents referred other potential respondents to the study. Only completed questionnaires were included in the research.

Questions about technical controls, monitoring and accountability were generated by the authors. To measure stress, the Perceived Stress Scale (PSS) was used. PSS was developed by Cohen and Williamson (1988); it is a Likert-type scale with 10 items and answer options of 0 (never), 1 (almost never), 2 (sometimes), 3 (fairly often) and 4 (very often). To measure the stress, 14 items from the 20-item Individual Workplace Questionnaire (IWQ) (Koopmans et al., 2012) were used. The IWQ is a Likert-type scale with answer options of 0 (never), 1 (rarely), 2 (sometimes), 3 (regularly) and 4 (often).

The main analytical method was mediation analysis. This technique is employed to "understand a known relationship by exploring the underlying mechanism or process by which one variable influences another variable through a mediator variable" (MacKinnon et al., 2007), and was therefore perfectly suited to this study of stress as a mediator of between technical controls, accountability, monitoring and job performance.

5.1   Statistical Analysis

Statistical Package for Social Sciences (SPSS; version 25) was used to analyse the descriptive statistics of the study variables and demographics. The outliers of the data were also checked and fixed. Cronbach's alpha was calculated to check the reliability of the scales. Mediation analysis was run using Hayes' (2018) PROCESS v3.3 macro in SPSS. The alpha level was set at 0.05 in this study.

6   Results

From all the distributed surveys, 302 complete surveys were obtained, with a response rate of 91%. The respondents had diverse characteristics with 70% males (211) and 30% females (91), and over half of the participants, i.e., 66 %, were aged between 18–30 years. All participants had at least graduation level

education. Most of the participants, i.e., 71.1%, had more than five years of work experience, and mostly experienced in the IT/ Computer field, i.e., 56%. They worked in different Saudi organisations located across Saudi Arabia.

6.1 Descriptive Statistics

This section presents the overall descriptive statistics and then the results of mediation analysis. Table 1 below presents the psychometric properties and descriptive statistics of the major study variables.

Table 1 - Psychometric properties of the major variables (N=302)

Variables	K	α	M	SD	Skewness	Kurtosis
Accountability	10	.83	4.33	.50	-1.41	2.39
Monitoring	10	.77	4.32	.44	-1.90	1.42
Technical controls	6	.70	4.35	.53	-2.88	2.04
Stress	10	.87	4.33	.54	-1.24	.47
Job Performance	14	.92	2.31	.80	.83	1.01

Note: K=no. of items of the scale, α=Cronbach's alpha, M=mean, SD=standard deviation.

Table 1 shows that the data is almost normally distributed, with variable skewness and kurtosis ranging between +3 and -3 (Brown & Venkatesh, 2005). Cronbach's alpha indicates that all scales y had good reliability values. Of all the scales, the job performance scale (i.e., the 14 items from the IWQ) had the highest reliability.

6.2 Mediation Analysis

The direct, indirect, and independent effects of the independent variables on the dependent variable were determined and are shown in the three models below.

6.2.1 Model 1: Accountability, Stress and Job Performance

In model 1, accountability was an independent variable, stress was a mediator and job performance the outcome variable (Fig. 2).
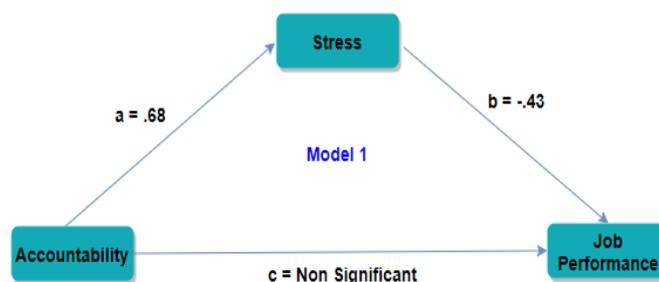
Figure 2 - Accountability, stress, and job performance

The results of the regression analysis indicated that the path (direct effect) from accountability to stress was positive and statistically significant (a= 0.68, SE = 0.06, p<0.001), indicating that people who scored higher on accountability experienced higher stress than participants who scored lower on the measure. The path from stress to job performance (b) was significant and negative (b= -0.43, SE = 0.13, p=0.001), meaning that higher stress leads to lower job performance and vice versa. In contrast, the path from accountability to job performance was non-significant, indicating that there is no direct relationship between accountability and job performance (Fig 2), but there is an indirect relationship mediated by stress.

6.2.2 Model 2: Monitoring, Stress and Job performance

In model 2, monitoring was the independent variable, stress was the mediator and job performance the dependent variable, as Figure 3 shows.
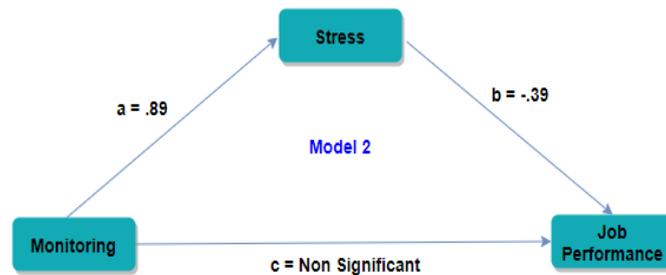
Figure 3 - Monitoring, stress, and job performance

The results of the regression analysis showed that the path (direct effect) from monitoring to stress was positive and statistically significant (a= 0.89, SE = 0.05, p<0.001), which supports the inference that people who experience high monitoring are prone to experience high. Moreover, the path from stress to job performance in model 2 (b) is negative and significant (b= -0.39, SE = 0.18, p=0.02), meaning that higher stress leads to low job performance and vice versa. The results showed no significant direct effect of monitoring on job performance (Figure 3).

The indirect effect (IE) was tested as in model 1, and was statistically significant (IE= -0.39, 95% CI -0.67, -0.08). The results depict a negative indirect relationship between accountability and job performance, meaning that stress plays a mediating role.

6.2.3 Model 3: Technical controls, Stress and Job Performance

Model 3 tested the effect of monitoring on job performance with and without the role of stress as a mediator (Fig. 4).
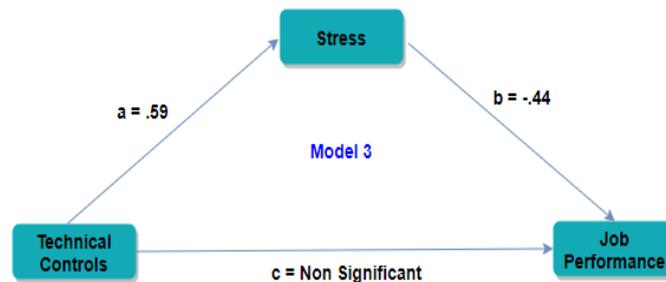
Figure 4 - Technical controls, stress, and job performance

The path (direct effect) from technical controls to stress was positive and highly significant (a= 0.59, S.E.= 0.06, p<0.001), supporting the assumption that people working under enforced technical controls have high potential to develop stress. Furthermore, the path from stress to job performance in model 3 (b) is negative and significant (b= -0.44, S.E.= 0.12, p<0.001), indicating that stress developed due to enforcement of technical controls leads to low job performance (Fig. 4). The results also show a non-significant relationship between technical controls and job performance.

The indirect effect in model 3 was tested the same way as previously and was found to be statistically significant (IE= -0.26, 95% CI 0.47, -0.07). Hence, stress plays a mediating role in the relationship between technical controls and job performance for the employees who participated in this study.

7   Discussion

In this section, the results of the study are discussed in relation to the hypotheses and the literature.

H1: Accountability is a significant predictor of stress among employees implying that increased perception of accountability may decrease performance of the employees.

Analysis indicated a significant positive relationship between accountability and stress, confirming H1. It is well understood that people made accountable for certain tasks will be more stressed until the tasks are completed successfully. For some people, this stress hinders their social, academic or occupational performance, and their interpersonal relationships as well (Van Praag, 2004).

These results align with those of Furnell and Thomson (2009), who found that accountability can cause security fatigue and anxiety among employees. Although accountability is an important factor for organisational success (Lerner & Tetlock, 1999), a high level of accountability can create decision stress

(Siegel-Jacobs & Yates, 1996) and negate the effects of technical controls by reducing employees' compliance intention (Adelberg & Batson, 1978).

H2: *Monitoring coupled with accountability has a significant relationship with stress implying that if monitoring increases employee's stress also increases which may ultimately effect job performance of the employees.*

Hypothesis 2 was proved correct in mediation analysis. A direct relationship existed between monitoring and stress in this study, similar to Bradley's (2004) finding that monitoring and stress are highly correlated, as well as the outcomes of Aiello and Kolb's (1995) laboratory-based study of monitored and unmonitored employees. Monitoring is undoubtedly a useful management tool but can pose a mental threat to employees.

H3: *Enforced technical security controls cause stress that leads to low work performance.*

The results of the current study indicate that H3 is correct. This is in line with the work of D'Arcy et al. (2014), who found that enforcement of security protocols can limit employees' control over software or hardware, causing frustration and stress. Similarly, Roshidi Hassan (2014) found that employees of IT companies have lower job satisfaction than employees of other types of companies due to enforcement of technical controls.

H4: *Stress has a significant impact on employees' job performance*

The results of models 1, 2 and 3 show that stress caused by accountability, monitoring and technical controls had a significant negative relationship with job performance, confirming H4. In line with the current study, Jamal (1984) found a negative linear relationship between stress and job performance of employees; the research results reported by Affleck (1999) and AbuAlRub (2004) also supported the idea that stress lowers job performance.

H5: *There is an indirect relationship between accountability, monitoring, technical controls, and job performance implying that's stress plays a mediating role among this relationship.*

The study found an indirect relationship between accountability, monitoring and technical controls with job performance, with stress playing a mediating role, confirming H5. D'Arcy et al. (2014) similarly identified that technical controls enforced on the employees heightened stress among employees and that this decreased job performance. Likewise, Aiello and Kolb (1995) reported that monitoring of employees caused stress which lowered job performance.

From the literature review and discussions, most of the cited literature is quite old. The significant difference between those studies and this current study is the collaborative study that has been performed here. None of the previous papers have discussed the factors in terms of cyber security and stress they are inducing in the cyber security context. Most of the literature assessing the inducing of stress in organizational environments are focused on accountability. The Technical controls and monitoring are mostly overlooked. For example, in (Adelberg & Batson, 1978) the author set up an experiment for the assessment of accountability in the university environment. The study was directly focused on financial accountability. Same as (Adelberg & Batson, 1978), mostly all studies are conducted in a non-cyber security context. Furthermore, this study assesses the mediating effect of stress on job performance. Therefore, this study is more extensive in terms of the variables and relationships assessed. To the best of our knowledge, this is one of the first studies that directly focuses on the impact of technical controls, accountability, and monitoring on employee job performance by assessing the mediating role of stress.

8 Conclusion

The main aim of the current research was to determine whether stress has a mediating effect on the relationship between three independent variables (accountability, monitoring and technical controls) and the outcome of job performance. Although previous researchers had studied the relationship of accountability and monitoring with job performance (Chen et al., 2012; CommandHound, 2019; Feigenbaum et al., 2011; Liu et al., 2021; Vance et al., 2013), very few had characterised the mediating effect of stress in these direct relationships. Similarly, the effect of technical controls has not been analysed in any previous research. And specially the role of these variables, i.e., technical controls, accountability, and monitoring with respect to cyber security and stress were not studied in previous research. the current research fills this gap.

The main implications of the research findings are for the IT and security sectors of organisations. Burdening employees with extensive technical controls, along with continuous monitoring and high

accountability creates stress that can be counterproductive. Hence, business owners and policymakers must design rules for deploying technical controls, monitoring and accountability for cyber security compliance that minimise their effect on employee's stress in the interests of maintaining job performance.

This research is lacking generalisability because of lack of random sampling and restriction to Saudi Arabian employees. Future research could take a larger sample from employees from more diverse sociocultural backgrounds to identify the mediating effects of stress on the relationship between cyber security technical controls, monitoring and accountability on job performance.

9 References

AbuAlRub, R. F. (2004). Job stress, job performance, and social support among hospital nurses. In *Journal of Nursing Scholarship*. https://doi.org/10.1111/j.1547-5069.2004.04016.x

Adelberg, S., & Batson, C. D. (1978). Accountability and helping: When needs exceed resources. *Journal of Personality and Social Psychology*. https://doi.org/10.1037/0022-3514.36.4.343

Affleck, M. A. (1999). Stress and Job Performance: Theory, Research, and Implications for Managerial Practice. *The Journal of Academic Librarianship*. https://doi.org/10.1016/s0099-1333(99)00113-5

Aiello, J. R., & Kolb, K. J. (1995). Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress. *Journal of Applied Psychology*. https://doi.org/10.1037/0021-9010.80.3.339

Alder, G. S. (2001). Employee reactions to electronic performance monitoring: A consequence of organizational culture. *Journal of High Technology Management Research*. https://doi.org/10.1016/S1047-8310(01)00042-6

Alqahtani, M. S., & Erfani, E. (2021). Exploring the Relationship Between Technology Adoption and Cyber Security Compliance: A Quantitative Study of UTAUT2 Model. *International Journal of Electronic Government Research (IJEGR)*, *17*(4). https://doi.org/10.4018/IJEGR.2021100103

Ament, C., & Haag, S. (2016). How information security requirements stress employees. *2016 International Conference on Information Systems, ICIS 2016*.

Amin, H. (2019, December 3). *How to Create a Culture of Accountability in the Workplace*. https://soapboxhq.com/blog/management-skills/create-culture-accountability-workplace

Baltaş, A., & Baltaş, Z. (1993). Stres ve Başa Çıkma Yolları. In *Remzi Kitabevi 14. Basım. İstanbul*.

Brown, S. A., & Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. In *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/25148690

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/25750690

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*. https://doi.org/10.2753/MIS0742-1222290305

Christina, N. K. and O., Cox, T., & Griffiths, A. (1996). Work-related stress in nursing : Controlling the risk to health. *Health Science Journal*.

Cohen, S., & Williamson, G. (1988). Perceived stress in a probability sample of the United States. In *The Social Psychology of Health*.

CommandHound. (2019). *Accountability Is Key to Security, Quality, and Compliance*. https://www.commandhound.com/accountability/accountability-is-key-to-security-quality-compliance/

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*. https://doi.org/10.1111/isj.12319

Cukier, M. (2016). *Study: Hackers Attack Every 39 Seconds | A. James Clark School of Engineering,*

University of Maryland. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management and Computer Security*. https://doi.org/10.1108/IMCS-08-2013-0057

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*. https://doi.org/10.2753/MIS0742-1222310210

D'urso, S. C. (2006). Who's watching us at work? Toward a structural-perceptual model of electronic monitoring and surveillance in organizations. *Communication Theory*. https://doi.org/10.1111/j.1468-2885.2006.00271.x

Dempsey, K. L., Chawla, N. S., Johnson, L. A., Johnston, R., Jones, A. C., Orebaugh, A. D., Scholl, M. A., & Stine, K. M. (2011). Information Security Continuous Monitoring (ISCM) for federal information systems and organizations. In *NIST Special Publication - 800 series*.

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Feigenbaum, J., Hendler, J. A., Jaggard, A. D., Weitzner, D. J., & Wright, R. N. (2011). Accountability and deterrence in online life (extended abstract). *Proceedings of the 3rd International Web Science Conference, WebSci 2011*. https://doi.org/10.1145/2527031.2527043

French, J. R. P., Rodgers, W., & Cobb, S. (1974). Adjustment as person-environment fit. In *Coping and adaptation*.

Furnell, S., & Thomson, K. L. (2009). Recognising and addressing "security fatigue." *Computer Fraud and Security*. https://doi.org/10.1016/S1361-3723(09)70139-3

Gordon, R. A., Rozelle, R. M., & Baxter, J. C. (1989). The effect of applicant age, job level, and accountability on perceptions of female job applicants. *Journal of Psychology: Interdisciplinary and Applied*. https://doi.org/10.1080/00223980.1989.10542962

Harris, M. A., & Martin, R. (2019). *Promoting Cybersecurity Compliance* (pp. 54–71). https://doi.org/10.4018/978-1-5225-7847-5.ch004

Hayes, A. F. (2018). Introduction to Mediation, Moderation, and Conditional Process Analysis, Second Edition: A Regression-Based Approach. In *the Guilford Press*.

Jamal, M. (1984). Job stress and job performance controversy: An empirical assessment. *Organizational Behavior and Human Performance*. https://doi.org/10.1016/0030-5073(84)90009-6

Jamal, M. (2007). Job stress and job performance controversy revisited: An empirical examination in two countries. *International Journal of Stress Management*. https://doi.org/10.1037/1072-5245.14.2.175

Kiziloglu, M. (2018). A RESEARCH ON THE RELATIONSHIP BETWEEN WORKPLACE MONITORING AND JOB STRESS. *JOURNAL OF ORGANIZATIONAL BEHAVIOR RESEARCH*.

Koopmans, L., Bernaards, C., Hildebrandt, V., Van Buuren, S., Van Der Beek, A. J., & de Vet, H. C. w. (2012). Development of an individual work performance questionnaire. *International Journal of Productivity and Performance Management*. https://doi.org/10.1108/17410401311285273

Lambert, W. W., & Lazarus, R. S. (1970). Psychological Stress and the Coping Process. *The American Journal of Psychology*. https://doi.org/10.2307/1420698

Langford, D., Fellows, R. F., Hancock, M. R., & Gale, A. W. (2020). Organizational behaviour. In *Human Resources Management in Construction*. https://doi.org/10.4324/9781315844695-9

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers and Security*. https://doi.org/10.1016/j.cose.2016.02.004

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. In *Psychological Bulletin*. https://doi.org/10.1037/0033-2909.125.2.255

Liu, C., Liang, H., Wang, N., & Xue, Y. (2021). Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender. *Information Technology and People*. https://doi.org/10.1108/ITP-09-2019-0452

MacKinnon, D. P., Fairchild, A. J., & Fritz, M. S. (2007). Mediation analysis. *Annual Review of Psychology*. https://doi.org/10.1146/annurev.psych.58.110405.085542

Majumdar, P. (2020). *How Employee Monitoring can Enhance your Data Security Plan?* https://www.nucleustechnologies.com/blog/how-employee-monitoring-can-enhance-your-data-security-plan/

Park, H. J., & Cho, J. S. (2016). The influence of information security technostress on the job satisfaction of employees. *Journal of Business and Retail Management Research*.

Polat, N. (Başkent U. I. of S. S. (2008). *Stress and Job Satisfaction Due to Work in Nurses: Field Study in A Training Hospital*.

Ponemon, L. (2019, July 23). *What's New in the 2019 Cost of a Data Breach Report*. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

Ragu-Nathan, T. S., Tarafdar, M., & Tu, Q. (2008). *The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation*. https://doi.org/10.1287/isre.1070.0165

Risk Based Security. (2019). *2019 on track to being the "worst year on record" for breach activity*. https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Roberts, B. W. (2003). Organizational Behavior Management and Personality Psychology. *Journal of Organizational Behavior Management*. https://doi.org/10.1300/j075v22n02_06

Rodell, J. B., & Judge, T. A. (2009). Can "Good" Stressors Spark "Bad" Behaviors? The Mediating Role of Emotions in Links of Challenge and Hindrance Stressors With Citizenship and Counterproductive Behaviors. *Journal of Applied Psychology*. https://doi.org/10.1037/a0016752

Roshidi Hassan. (2014). Factors Influencing Turnover Intention Among Technical Employees in Information Technology Organization : a Case of Xyz (M) Sdn . Bhd. *International Journal of Arts and Commerce*.

S. Raschid Muller, & Mary L. Lind. (2020). Factors in Information Assurance Professionals' Intentions to Adhere to Information Security Policies. *International Journal of Systems and Software Security and Protection (IJSSSP)*, *11*(1). https://doi.org/10.4018/IJSSSP.2020010102

Siegel-Jacobs, K., & Yates, J. F. (1996). Effects of procedural and outcome accountability on judgment quality. *Organizational Behavior and Human Decision Processes*. https://doi.org/10.1006/obhd.1996.0001

Thoms, P., Dose, J. J., & Scott, K. S. (2002). Relationships between accountability, job satisfaction, and trust. *Human Resource Development Quarterly*. https://doi.org/10.1002/hrdq.1033

Toth, P., Klein, P., Toth, P., & Klein, P. (2014). A Role-Based Model for Federal Information Technology / Cybersecurity Training NIST Special Publication 800-16 A Role-Based Model for Federal Information Technology / Cybersecurity Training. *Nist Sp 800-16*.

Van Der Doef, M., & Maes, S. (1999). The Job Demand-Control(-Support) model and psychological well-being: A review of 20 years of empirical research. *Work and Stress*. https://doi.org/10.1080/026783799296084

Van Praag, H. M. (2004). Can stress cause depression? In *Progress in Neuro-Psychopharmacology and Biological Psychiatry*. https://doi.org/10.1016/j.pnpbp.2004.05.031

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*. https://doi.org/10.2753/MIS0742-1222290410

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*. https://doi.org/10.1016/j.im.2012.04.002

Viner, R. (1999). Putting stress in life: Hans selye and the making of stress theory. *Social Studies of Science*. https://doi.org/10.1177/030631299029003003