Are External Auditors Capable of Dealing with Cybersecurity Risks?

Yueqi Li(✉), Sanjay Goel, and Kevin Williams

State University of New York at Albany, Albany, NY 12222, USA
yli69@albany.edu

Abstract. Cyber risk presents a significant threat to financial reporting systems and capital markets, regulatory authorities expect external auditors to obtain the competence necessary to deal with cyber risk. As an exploratory study, we aim to address the urgent question that whether current external financial auditors can deal with cybersecurity-related tasks, as well as what drives their performance in these emerging tasks related to cybersecurity. Based on the survey data of external auditors from accounting firms located in Shanghai, China, we found that these auditors did not consistently understand fundamental concepts related to cyber risk. Using partial least squares based structural equation modeling, results indicate that the personality trait of openness to experiences positively, while operating stress negatively impact auditor performance in cybersecurity. Auditors' risk attitudes did not show significant influence on their cybersecurity performance. These findings can be used as a new source for regulators, researchers, and practitioners in their efforts of identifying audit quality drivers in the changing environments.

Keywords: External Auditor · Cybersecurity Performance · Personality · Operating Stress · Risk Attitudes

1 Introduction

In recent years, cyberattacks have become unprecedented, and cybersecurity has become critical to the success of businesses. According to China's National Internet Emergency Center, there were 23.07 million malicious programs, 13, 083 security breaches, over 13, 000 spoofing websites during the first half year of 2021 (National Internet Emergency Center 2021). A Chinese technology risk expert at Deloitte, China suggested seven hidden costs of a cyberattack, including disruption or damage to business operations, loss of customers, loss of contract revenue and the added value, devaluation of the trademark, reputation damage, intellectual property damage, and potential cybersecurity insurance costs (Xue 2017). External auditors, who provide assurance over companies' financial reporting, has been expected to consider cybersecurity risks in their operations.

Today, accounting regulators and standards-setters are concerned about whether companies and auditors are paying enough attention to cyber risks and related disclosures (International Organization of Securities Commissions (IOSCO) 2016; Li et al. 2020;

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 326–340, 2023.
https://doi.org/10.1007/978-3-031-36574-4_19

PCAOB 2014; Securities and Exchange Commission (SEC), 2014, 2018). According to AICPA 2021 exam blueprints, CPAs should be able to identify the risks associated with protecting sensitive and critical information within information systems (AICPA, 2021). In the Chinese Institute of Certified Public Accountants (CICPA)'s CPA Industry Informatization Construction Plan 2021–2025, CICPA highlighted the importance and necessity of implementing cybersecurity education in the CPA profession (CICPA 2021). To address regulatory concerns, auditors have increased their audit risk awareness and put adequate procedures in place to deal with the consequences of cybersecurity incidents (Rosati et al. 2019), and accounting firms have established cybersecurity service lines. However, these classically trained auditors may not be adequately equipped to perform cybersecurity-related tasks. Whether auditors can deal with cybersecurity-related tasks remains a critical and urgent question.

This current study aims to understand how skilled auditors are in dealing with cyber risk and what affects their capability of conducting cybersecurity-related tasks. External auditors who work in accounting firms and perform auditing services for their clients are increasingly expected to assess cybersecurity risk and its impact on financial reporting. We use a sample of Chinese external auditors to assess external auditors' performance in cybersecurity related tasks and explores factors that affect their performance in cybersecurity performance. We found that these traditional financial auditors did not consistently understand cybersecurity basics, which call for extended and systematic cybersecurity training in the audit profession. The personality of openness to experience and operating stress both significantly affect auditors' cybersecurity performance. These findings will inform audit leaders in their efforts of personnel management, as well as audit regulators in their efforts of identifying audit quality drivers.

2 Background

2.1 Cybersecurity Regulations in Accounting

As cyber risk presents a growing threat to the financial reporting system and capital markets, many accounting regulatory authorities have addressed concerns and developed frameworks regarding cyber risk. The SEC emphasized the responsibilities of management and boards regarding cybersecurity and provide guidance in assisting public companies to prepare for their disclosures about cybersecurity risks and incidents in its *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (SEC 2018). The PCAOB specifically alerts external auditors to consider how cyber incidents might affect a firm's internal control over financial reporting (ICFR) (PCAOB 2010). In April 2017, the American Institute of Certified Public Accountants (AICPA) introduced a market-driven, flexible, and voluntary cybersecurity risk management reporting framework that highlights the importance of security/cybersecurity attestation in organizations (AICPA 2017a). The AICPA has also developed guidance for certified public accountants (CPAs) to help manufacturers and distributors better understand cybersecurity risks in their supply chains (AICPA 2018). The Financial Industry Regulatory Authority (FINRA) offered two studies on best practices for cybersecurity—FINRA (2015) covers overall cybersecurity issues; FINRA (2018) is targeted to particularly significant concerns and specifically addresses cybersecurity controls. The

Committee on Payments and Market Infrastructures and the Board of the IOSCO released the *Guidance on Cyber Resilience for Financial Market Infrastructures,* which is the first internationally agreed-upon guidance on cybersecurity targeting the financial industry (IOSCO, 2016).

China released *Cybersecurity Law of the People's Republic of China (2016 CSL, with effect from 1 June 2017)* in 2016 to promote cybersecurity and maintain cyberspace in the nation (Cybersecurity Law of the People's Republic of China, 2016). In the Chinese Institute of Certified Public Accountants (CICPA)'s *CPA Industry Informatization Construction Plan 2021–2025,* CICPA highlighted the importance and necessity of implementing cybersecurity education in the CPA profession (CICPA 2021). Researchers at the National Audit Office in China proposed that the cybersecurity audits should include the assessment of the cybersecurity risks faced by the organization and the assessment of whether their cybersecurity protection measures can effectively address the cybersecurity risks (Chen and Sui 2019), their work focuses on the cybersecurity audits for government agencies. Cyberspace Administration of China (CAC) released *Regulations on Network Data Security Management (Draft fort Comments)* in 2021, which first proposed a data security audit system (No. 58). The system provides two types of data security audits: 1) the self-audit requires the data processor to hire the data security audit professionals to carry out regular compliance audits on their personal data handling; 2) the examination audit requires managers and supervisory departments to carry out audits on important data processing activities (CAC 2021).

2.2 Auditors' Role in Cyber Risk

According to the CICPA, auditors work as independent third parties to express an opinion on financial statements being audited. To fulfill their roles, auditors shall comply with the code of professional ethics, plan and perform audits according to the requirements of auditing standards, obtain sufficient and appropriate evidence, and draw a reasonable audit conclusion based on the audit evidence obtained (CICPA 2006). Over the last two decades, auditing markets in China are dominated by "Big Four" accounting firms. The nature of the external audit services and the definition of audit quality does not vary between China and foreign countries (Zhou and Lv 2007).

Many accounting regulatory authorities and academic research have defined individual auditors' and audit firms' role with respect to cybersecurity. Their expected auditors' responsibilities in regard to cybersecurity have been summarized as follows:

Auditors are expected to:

- Consider cybersecurity risk in their operations (CAQ 2018);
- Identify cybersecurity risks associated with protecting critical and sensitive information within information systems (AICPA 2021; CICPA 2021);
- Focus on the information technology (IT) that a public company uses to prepare its financial statements and automated controls around financial reporting (PCAOB 2010);
- Evaluate whether financial statements are presented fairly under the applicable accounting principles as a whole and if the financial statements reflect cybersecurity-related incidents (PCAOB 2009; Knechel 2021);

- Review clients' cybersecurity disclosures and other cybersecurity related information in financial reports (CAQ 2018; Calderon and Gao 2020; Knechel 2021);
- Understand the controls in place and the methods used to prevent and detect cyber incidents that may materially affect a company's financial reporting (Hamm 2019);
- Understand management's approach to cybersecurity risk management (CAQ 2018);
- Assist boards of directors in their oversight of cybersecurity risk management (CAQ, 2018);
- Audit firms are expected to perform cybersecurity-related advisory, assurance, and audit services (Eaton et al. 2019).

To date, external auditors' ability of dealing with cybersecurity-related tasks is not well understood and evaluated in the current state of research. There has been no clear description on external financial auditors' responsibility relating to cybersecurity. In this study, we specifically focus on external auditors' performance in understanding and identifying cybersecurity risks, which is fundamental to their roles surrounding cybersecurity subject matter. The dependent variable in this study is external auditors' performance in cybersecurity. Consistent with the latest AICPA and CICPA's exam requirements for CPA candidates, we define auditors' performance in cybersecurity as their performance in identifying cybersecurity risks associated with protecting sensitive and critical information (AICPA 2021; CICPA 2021).

3 Hypotheses

3.1 Personality of Openness

The extant cybersecurity and auditing literature has examined the personality characteristics of external auditors (Dewi and Dewi 2018; Samagaio and Felício 2022). Barrick and Mount (1991) found that the openness trait has a positive effect on performance. Openness to information, experience, or being open to new things is a personality dimension that categorizes people based on their interest in new things, creativity, imagination, and high intelligence (Kumar and Bhakshi 2010). As one of the five personality traits within Big Five Personality Model (BFM) (Cherry 2021; Robbins and Judge, 2008), the openness captures one's attitudes towards emerging subjects. Cybersecurity-related tasks are relatively new to traditional financial auditors. The current external auditors of financial statements are mostly experts of financial accounting and auditing with few backgrounds of cybersecurity, which makes cybersecurity-related tasks challenging to traditional external auditors. Rustiarini (2013) found that external auditors with a high openness personality can overcome problems in a short time, with limited information, and under high uncertainty, which leads auditors to perform better on the tasks they are unfamiliar with, like cybersecurity-related tasks. Therefore, auditor with higher openness characteristic is likely to be associated with a higher level of professional skepticism employed in an emerging task, which leads to improvement in their cybersecurity performance. To date, how openness affects external auditors' performance in dealing with emerging tasks, such as cybersecurity-related tasks, have not been studied.

Therefore, it is hypothesized that higher openness personality is correlated with better auditors' performance in assessing cyber risk.

H1: Openness to experience significantly and positively predicts an auditor's performance in cybersecurity.

3.2 Risk Attitudes

Auditors' attitudes constitute components of their feelings and beliefs about risk (Nolder and Kadous 2018). Risk attitudes, which are described as a "chosen state of mind with regard to those uncertainties that could have a positive or negative effect on objectives" (Hillson and Murray-Webster 2006, p. 4), are an important aspect of external auditors' attitudes in risk assessment tasks. Clarke (1987) showed that significant systematic differences exist among auditors regarding individual risk attitudes and perception biases and that auditors' risk attitudes affect their decisions of the audit scope. Risk attitudes also refer to risk appetite (i.e., risk-averse, risk-neutral, or risk-prone) (Farmer 1993), or risk capacity (Hindson 2013). People who are classified as risk-averse have a lower risk tolerance and are likely to see an event as risky. The majority of audit firms agree that Big Four firms are more risk-averse with respect to the reputation damage from public scandals and/or audit failures (Sawan and Alsaqqa 2013). Research findings also suggest that audit partners that are more risk-prone conduct lower quality audits; the clients of more risk-prone partners are more likely to misstate, pay lower audit fees, and less timely recognize loss (Pittman et al. 2019). In terms of individual auditors, auditors who are risk-averse tend to express a more severe audit opinion (Breesch and Branson 2009). Auditors who are detailed processors that read all of the available information tend to process more risk cues before making their final judgment and be more aware of the dangers implied by these cues, which leads to more risk-averse judgments (Goldhaber and deTurck 1988). These dangers, which are cyber risks, are more likely to be identified and evaluated by risk-averse auditors. Therefore, a higher level of risk aversion can lead to a higher level of susceptibility to cyber risks.

H2: The level of risk aversion significantly and positively predicts an auditor's performance in cybersecurity.

3.3 Operating Stress

Auditors and cybersecurity professionals are operating under great pressure, given the complex and difficult nature of their tasks (Gaertner and Ruhe 1981). DeZoort and Lord (1997) (p. 33) defined auditors' job stress as "the stress caused by his or her self-perceived inability to perform well in an ongoing auditing work environment". Stress is generally recognized as being negatively associated with cognitive abilities, task effectiveness, and general well-being (Linden et al. 2005). While stress could to some extent lead to a higher work efficiency (DeZoort and Lord 1997; McDaniel 1990), the potential of pressure-induced dysfunctional behavior could lead to impaired auditors' job performance (DeZoort and Lord 1997; Smith et al. 2007). Given the high-risk and mission-critical nature of audit tasks, stress can be harmful to auditors in their daily operations. The excessive workload and mental stress could eventually prevent current auditors to commit themselves in emerging tasks, such as tasks related to cybersecurity domain. This current study applied the fatigue level (physical tiredness) and frustration

level (mental tiredness) to represent operating stress in the context of auditors' cybersecurity performance. Fatigue and frustration were proposed by Dykstra and Paul's (2018) Cyber Operation Stress Survey (COSS) as indicators of operating stress of cybersecurity professionals. When financial auditors experience a great workload and harsh work conditions, their fatigue levels tend to increase, which is likely to cause errors and lead to decreased performance (Li et al. 2013). Many factors that potentially lead to worker frustration include a lack of means and materials, inadequate work environments, deficits in human resource management, and opaque and unfair training opportunities (Mathauer and Imhoff 2006). This frustration demotivates workers from realizing their highest potential. Using fatigue and frustration to indicate both physical and mental tiredness would open up new approaches for job stress studies in the audit literature.

H3: Operating stress, indicated by fatigue level and frustration level, significantly and negatively predicts an auditor's performance in cybersecurity.

4 Research Methods

4.1 Sample

The sample for this research was composed of external auditors from accounting firms located in Shanghai, China[1]. The sampling was anonymous, and the researchers determined the admission of participants from the applicant pool using the following goals: auditors who work at public accounting firms or who have worked as auditors in public accounting firms within the past six months.

4.2 Data Collection

This study used primary data, which were collected by emailing anonymous survey links to the respondents. To recruit Chinese auditor participants, the snowball sampling technique was used in which research participants are asked to identify additional potential subjects for the research. The recruiting advertisement was sent to the group of auditor alumni via social media in Shanghai, and then the auditor alumni participated in the survey voluntarily and circulated the recruiting information among their auditor colleagues. These auditors are from 10 accounting firms, including both big accounting firms and local accounting firms. Most of them are from Big 4 accounting firms, including EY (34.5%) and KPMG (17.3%).

The questionnaire was translated by the author of this current study and validated by a Chinese faculty member who works in a prestigious U.S. educational institution and a Chinese audit professional who is proficient in English. Eligible auditors who applied to participate in this study were sent an anonymous link to the survey via email.

The total number of recorded responses is 69, with 37 of which are incomplete. The incomplete responses either did not approve the written information consent or left the cyber risk task unanswered. These incomplete responses are not paid, we only provided payments to people who answered all the required questions in the survey, and

[1] IRB exemption has been granted by the Institutional Review Board at the State University of New York (Study number: 20X242; date of approval: October 15, 2020).

we expect participants to be engaged while they participate in the survey. Finally, 32 out of 69 recorded questionnaires were considered complete and usable (see Table 1 for details). To calculate an acceptable sample size, we use parameter values of anticipated effect size of 0.35 (we anticipate a large effect), desired statistical power level of 0.8 and probability level of 0.05. The effect sizes that we obtained from regression analyses confirm that the predictors have a fairly large effect. In this study, we have total of four predictors, with two of which were retained after stepwise regression. Therefore, the acceptable sample size for the regression with four predictors is 39, the acceptable sample size for the regression with two predictors is 31. Therefore, our sample size is acceptable for our analyses.

Table 1. Details of Distribution and Recorded Questionnaires

Explanation	Amount	Percentage (%)
Recorded questionnaires	69	100.0
Canceled questionnaires (incomplete filling)	37	53.6
Used questionnaires	32	46.4
Valid response rate = 32/69 * 100% = 46.4%		

As an exploratory study, we mainly focus on addressing the current auditors' performance in the emerging cybersecurity-related tasks. Dealing with cybersecurity-related tasks poses some challenges for all the participating auditors, auditors in China generally have very busy schedule, both of which make it difficult to recruit them in the survey. However, we argue that understanding current auditors' performance in cybersecurity-related tasks is of great importance and urgence given the regulatory emphasis and the concerns from key stakeholders. We acknowledge that the respondents of convenience may not wholly represent the population of interest, which are current external auditors, but we eliminated bias as much as possible in the process of sampling and data collection. We anticipate this work to serve as a guiding resource for future studies both in China and internationally.

4.3 Measurement of Independent Variables

The personality trait of openness was tested following Goldberg's (1992) Big Five personality markers, which uses a publicly available source of the 50-item IPIP version of the Big Five Markers score the five personality traits. For this study, we only extracted the ten questions testing openness trait. For each question, participants rated their level of agreement from 1 to 5 (1 = strongly disagree, 5 = strongly agree). The level of risk aversion was used to represent risk attitudes. The Passive Risk-Taking Scale (Keinan and Bereby-Meyer, 2012) was used, in which 25 Likert questions are included (1 = strongly disagree, 7 = strongly agree).

Fatigue and frustration were tested using the question suggested in the Cyber Operations Stress Survey (COSS). To test fatigue and frustration level, auditors were given

seven progressive stages and asked to identify the stage that best fits their actual condition right before doing the cybersecurity task (Dykstra and Paul 2018, p. 8). Fatigue level is rated from "fully alert, wide awake" to "exhausted, unable to function effectively", while frustration level is rated from "very low" to "very high" on the question about "how insecure, discouraged, irritated, and annoyed are you right now." Both fatigue and frustration were tested immediately before and immediately after the cybersecurity task.

4.4 Measurement of Dependent Variable – Auditors' Performance in Cybersecurity

The dependent variable in this study is referred to as external auditors' performance in cybersecurity. To test the dependent variable, we used a case scenario task extracted from a cyber risk assessment case study developed by Ayo et al. (2018). Consistent with the latest CPA exam blueprint's requirement on future CPA's skills in identifying cybersecurity risks associated with protecting sensitive and critical information, we asked respondents to examine the case scenario and identify all the threats, vulnerabilities, and risks they perceive. Auditor performance is the action or execution of auditing tasks completed by an auditor within a certain period (Trisnaningsih, 2007). The measurement of an auditor's performance in the case scenario task was done according to an executive rubric developed by the authors of this current study and modified by an external cybersecurity risk assessment expert. The external cybersecurity expert also graded a few responses as sample gradings. Based on the rubric and the sample gradings, auditor performance was evaluated independently by two Ph.D. students with both CPA and cybersecurity backgrounds. They reached a consensus on each response and assign a final score for each response. Each auditor's performance in cybersecurity was scored numerically on a scale from 0 to 100, where 0 meant no relevant answers were provided, and 100 meant the performance was as good as the performance of a cybersecurity expert. All the instruments can be found in the Appendix.

The Ayo et al. (2018) case study is to provide a full cybersecurity risk assessment on an African company called "SparTax Collection Agency" based on some background scenario of the agency. To examine students' performance in cybersecurity, we extracted the background scenario of the agency, including its recent cybersecurity breach history in Africa, the major business that the agency does (i.e., to contracted by the Finance Authority of local governments to collect revenue in the form of taxes), implemented technologies and third-party contracted information systems, security policies, personnel, and organizational structure. We asked students to identify cybersecurity threats, vulnerabilities, and risks, should they exist. As CPA candidates and future accounting professionals, we expect them to 1) systematically distinguish the basic cybersecurity concepts (i.e., threats, vulnerabilities, and risks); 2) sufficiently identify cybersecurity threats, vulnerabilities, and risks that may exist for the agency; 3) look into cybersecurity issues from different aspects (e.g., cybersecurity risks emerged from security policies, personnel management, third parties, etc.); 4) and clarify the impact of each identified cybersecurity issues.

4.5 Analysis

The hypothesis testing in this research was done through partial least squares (PLS) based structural equation modeling (SEM). Previous studies have showed evidence for the validity of using PLS-based SEM for small sample sizes (Henseler et al. 2016; Reinartz et al. 2009; Rigdon 2016; Sarstedt et al. 2016). We employed partial least squares (PLS) based Structural Equation Modeling (SEM) to explore both the measurement model of operating stress and the structural model of cybersecurity performance.

5 Results

5.1 Descriptive Statistics

Among all the 32 participants, the average age was 24.5, and 16 *(50%)* of them are male. Participants have averagely been trained for cybersecurity for 19.66 h during the last year (2019–2020). 22 of the 32 participants *(68.8%)* have the highest educational degree as bachelor's, while the rest 10 of the 32 participants *(31.3%)* have a master's degree. Participants' experiences in the field of auditing run from a few months to 9 years, with a mean of 14.63 months. Therefore, our Chinese auditor sample consists of relatively newer auditors.

Overall, the respondents' openness level *($M = 24.38$, $SD = 4.95$)* and risk aversion level *($M = 87.84$, $SD = 18.21$)* are about the moderate level. On average, the respondents were between "very responsive, but not at the peak" and "okay, somewhat fresh" in terms of fatigue level and slightly low on frustration level *($M = 2.91$, $SD = 1.35$)* immediately before the cybersecurity task. After completing the cybersecurity task, participants' fatigue level *($MD = 0.66$, $p < .01$)* and frustration level *($MD = 0.44$, $p < .05$)* both significantly increased. The average performance score was not high *($M = 40.34$, $SD = 19.65$)*. On average, auditors were able to identify 5.47 items related to cybersecurity issues, while there were 24 significant possible cybersecurity threats and 24 significant vulnerabilities exist in the scenario (see Ayo et al. 2018). Most auditors were able to find cybersecurity issues related disgruntled employees, outdated security policies, insufficient security training for employees, and third-party risks, and cloud security. However, very few students explained why such cybersecurity issues may exist or illustrated the negative impacts. They were also not able to identify specific cybersecurity threats (e.g., SQL injections, social engineering, etc.) that are likely to occur for the agency.

The internal consistency reliability was acceptable for all scales (Cronbach's alpha was above 0.8) (Lance et al. 2006). None of the control variables was significantly correlated with performance or was sufficiently significant to enter the regression model at a significance level of .05, leading us to exclude them in both the correlation and regression analyses.

5.2 PLS-Based SEM Analyses

We used PLS-based structural equation modeling (SEM) to model the effects of openness personality, risk aversion, and operating stress indicators of fatigue and frustration on

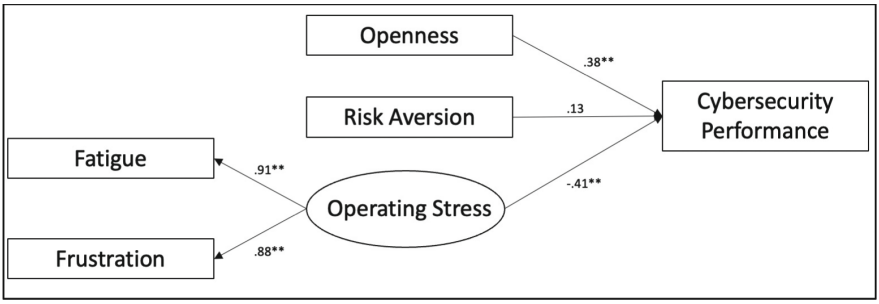

Fig. 1. PLS-based SEM Results

auditors' cybersecurity performance. The PLS-based SEM results are reflected in Fig. 1. The assumption of noncollinearity was met.

PLS-SEM requires a two-step approach in analyzing and interpreting a research model (Hair et al. 2017), including the measurement model and the structural model. The assessment of the measurement model requires the inspection of convergent validity and reliability (Hair et al. 2017, 2019). Convergent validity was analyzed using the standardized loadings of the indicators and the average variance extracted (AVE). We found fatigue and frustration both showed high standardized factor loadings (above 0.8), the average variance extracted (AVE) was above 0.8, indicating the model has convergent validity. Composite reliability (CR) was above the threshold of 0.70 (Hair et al. 2017), suggesting that all constructs have good reliability.

For the structural model, the personality of openness positively *($B = .38$, $p < .01$)*, while operating stress negatively *($B = -.41$, $p < .01$)* affect auditors' cybersecurity performance. The adjusted R-square is 0.423, indicating 42.3% variances in cybersecurity performance could be explained by the presented SEM-PLS model, showing high model predictive accuracy. The insignificant effect of risk aversion is consistent with our findings in stepwise regression analyses. We also run the effect size (f^2) to measure the effect of each performance driver. Using Cohen (1988) threshold, we found both openness *($f^2 = 0.245$)* and operating stress *($f^2 = 0.270$)* to have small to medium effects.

6 Discussion

6.1 Discussion of Findings

This study explores external auditors' performance in cybersecurity and how personality, risk attitudes, and operating stress affect such performance. According to the responses from the research participants, we can conclude that the auditors did not consistently understand the differences among the concepts of cybersecurity threats, vulnerabilities, and risks. Understanding the basic concepts of cybersecurity and cyber risk is fundamental when dealing with cybersecurity-related tasks in daily operations. The results show that the auditors lacked fundamental competence in identifying cyber risk. In addition, auditors' responses to cybersecurity tasks indicate that they are able to identify cybersecurity issues with personnel management, such as insufficient security training and

disgruntled employees, while few of them could extend their scope of assessment to governance structures, mission/business processes, enterprise architecture, information security architecture, facilities, equipment, system development life cycle processes, supply chain activities, and external service providers (National Institute of Standards and Technology (NIST), 2012).

Personality traits have long been ignored in the security and IT audit literature. We found openness significantly improves auditors' performance in assessing cyber risks, which lends support to Neuman et al.' s (1999) and Rustiarini's (2013) findings on openness and performance in auditing tasks. Openness is a typical trait of professionals in technology fields, especially cybersecurity (Freed 2014). Our findings support that openness is also an important trait that auditors should have to perform well in cybersecurity-related tasks. The personality trait of openness also tends to mitigate the level of frustration, according to the correlation analysis. An open and curious attitude enables individuals to more competently deal with emotion-eliciting situations, which contributes to their general capability of dealing with daily challenges effectively (van der Kaap-Deeder et al. 2021), which could explain the negative correlation between openness and frustration.

The findings suggest that operational stress, represented by fatigue and frustration, negatively affects auditor performance in cybersecurity. The findings are in line with Linden et al. (2005)'s finding that stress diminishes one's performance. Hopstaken et al. (2015) argues that fatigue reduces motivation for effortful activity and impairs task performance. Therefore, the severe negative impact of fatigue on auditor performance in cybersecurity may be due to fewer auditing efforts that auditors have employed during a task. The utilization of fatigue and frustration to indicate the personal tiredness at both physical and mental levels will open up new approaches for future studies of auditors' job stress. While the risk aversion did not significantly affect cybersecurity performance, this could be a result that auditors did not systematically understand the definition of cybersecurity basics. Hence, they fail to identify cybersecurity threats, vulnerabilities, and risks even though they are sensitive to risks in general.

6.2 Implications

The results of this study have implications for academics and practitioners. First, this paper enriches the existing literature uniquely by exploring factors personality of openness, risk aversion, and operating stress that affect auditors' performance in cybersecurity. This is a critical step toward improving auditors' performance in cybersecurity related tasks. The problem that current auditors are not capable of identifying cybersecurity risks and potentially other cybersecurity-related tasks calls for comprehensive training in the auditing profession and academics. Future research should consider how training can be appropriately designed and effectively implemented to facilitate auditors' adaption to cybersecurity-related tasks, especially for younger and entry-level auditors. While factors of operating stress can be managed through effective staffing and planning, it is obvious that personality cannot easily be changed. Fortunately, American colleges and accounting firms can use the resources from this study to discover students and professionals to fit their educational/recruiting objective or distribute cybersecurity related tasks within the audit team more appropriately (Aufman and Wang 2019). Third, the

operating stress indicators derived from cybersecurity performance literature opens up new approaches for future studies on auditors' job stress. Future research could continue to use fatigue and frustration levels in measuring audit professionals' operating stress. Fourth, these factors could be used as part of a quality control program to conduct post-audit reviews, which could improve external audit quality when cybersecurity-related tasks are involved (Stoel et al. 2012). Finally, regulators and policymakers can incorporate these factors into ongoing or new frameworks of audit quality drivers.

6.3 Limitations

While this study contributes to both academia and practice, it also has limitations. First, the small sample size and the use of convenience sample may introduce additional biases. Given a smaller number of predictors used in this study, and a larger effect size anticipated, we believe using of a small sample size will produce credible results. As an exploratory study, we mainly focus on addressing the urgent question regarding current auditors' performance in the emerging cybersecurity-related tasks. Dealing with cybersecurity-related tasks poses some challenges for all the participating auditors, auditors in China generally have very busy schedule, both of which have made it difficult to recruit current auditors in the survey. However, we argue that understanding current auditors' performance in cybersecurity-related tasks is of great interest to regulators, business leaders, accounting firms, and other key stakeholders. We have eliminated biases as much as possible in the process of sampling and data collection. We encourage future studies to use this study as a guiding resource and further explore how personality traits, attitudes, and operational stress affect external auditors' performance in emerging tasks related to cybersecurity, such as cyber risk identification, with a larger and random auditor sample. Second, it only focused on external auditors from accounting firms in China. Future studies may consider how these identified factors contribute to U.S. and other foreign external auditors' success in identifying cyber risks. Third, this study only measured the individual characteristics of external auditors; factors at the process, firm, and environmental levels should be further studied. In addition, the sample was comprised of relatively young auditors (see, e.g., Christensen et al. 2016); future studies should look at how these factors also work for the older population.

References

1. American Institute of Certified Public Accountants (AICPA): Description criteria for management's description of the entity's cybersecurity risk management program (2017a)
2. American Institute of Certified Public Accountants (AICPA): Enhancing audit quality. American Institute of Certified Public Accountants, New York, NY (2017b)
3. American Institute of Certified Public Accountants (AICPA): Information for entity management (2018)
4. American Institute of Certified Public Accountants (AICPA): Uniform CPA Examination® Blueprints (2021)
5. Aufman, S., Wang, P.: Discovering student interest and talent in graduate cybersecurity education. Adv. Intell. Syst. Comput. **800** Part F1 (2019)

6. Ayo, S.C., Ngala, B., Amzat, O., Khoshi, R.L., Madusanka, S.I.: Information security risks assessment: A case study. Cornell University (2018)
7. Barrick, M.R., Mount, M.K.: The Big Five personality dimensions and job performance: a meta-analysis. Pers. Psychol. **44**(1), 1–26 (1991)
8. Breesch, D., Branson, J.: The effects of auditor gender on audit quality. IUP J. Account. Res. Audit Pract. **8** (3/4) (2009)
9. Calderon, T.G., Gao, L.: Cybersecurity risks disclosure and implied audit risks: evidence from audit fees. Int. J. Audit. **25**(1), 24–39 (2020)
10. Chen, Y., Sui, X.: Research on Chinese government cybersecurity protection and auditing methods (2019)
11. CICPA: Objectives and general principles of the audit of financial statements (2006). https://www.cicpa.org.cn/news/newsaffix/7699_2006817_21.pdf. Accessed 15 Aug 2022
12. CICPA: Construction of cybersecurity ensures data security and business continuity. China Accounting News (2021). https://www.cicpa.org.cn/xxfb/Media_Fax/202106/t20210617_62435.html. Accessed 15 Aug 2022
13. Clarke, D.: An Examination of the Impact of Individual Risk Attitudes and Perceptions on Audit Risk Assessment. ProQuest Dissertations Publishing (1987)
14. Cohen, J.: Statistical Power Analysis for the Behavioral Science. Lawrence Erlbaum, Mahwah (1988)
15. Cyberspace Administration of China: Cybersecurity Law of the People's Republic of China (2016). http://www.cac.gov.cn/2016-11/07/c_1119867116.htm. Accessed 15 Aug 2022
16. Cyberspace Administration of China: Regulations on Network Data Security Management (Draft fort Comments), Pub. L. No. 58 (2021). http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm. Accessed 15 Aug 2022
17. Deloitte LLP: Advancing quality through transparency. Deloitte LLP Inaugural Report (2010)
18. Dewi, I.G.A.A.P., Dewi, P.P.: Big five personality, ethical sensitivity, and performance of auditors. Int. Res. J. Manage. IT Soc. Sci. **5**(2), 195–209 (2018)
19. DeZoort, F.T., Lord, A.T.: A review and synthesis of pressure effects research in accounting. J. Account. Lit. **16**, 28 (1997)
20. Dykstra, J., Paul, C.L.: Cyber operations stress survey (COSS): studying fatigue, frustration, and cognitive workload in cybersecurity operations (2018)
21. Eaton, T.V., Grenier, J.H., Layman, D.: Accounting and cybersecurity risk management. Current Issues in Auditing (2019)
22. Farmer, T.A.: Testing the effect of risk attitude on auditor judgments using multiattribute utility theory. J. Acc. Audit. Financ. **8**(1), 91–110 (1993)
23. Financial Industry Regulatory Authority (FINRA): Report on Cybersecurity Practices, Cybersecurity Investor Alert (2015). http://bit.ly/2W3B 1N1. Accessed 15 Aug 2022
24. Financial Industry Regulatory Authority (FINRA): Report on Selected Cybersecurity Practices (2018). http://bit.ly/2MuW9MK. Accessed 15 Aug 2022
25. Gaertner, J.F., Ruhe, J.A.: Job-related stress in public accounting: CPAs who are under the most stress and suggestions on how to cope. J. Account. **151**(June), 68–74 (1981)
26. Goldberg, L.R.: The development of markers for the Big-Five factor structure. Psychol. Assess. **4**, 26–42 (1992)
27. Goldhaber, G.M., deTurck, M.A.: Effectiveness of warning signs: gender and familiarity effects. J. Prod. Liability, **11**(3) (1988)
28. Hair, J., Hult, T., Ringle, C., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd edn. Sage Publication, California (2017)
29. Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M.: When to use and how to report the results of PLS-SEM. Eur. Bus. Rev. **31**(1), 2–24 (2019)

30. Hamm, K.M.: Cybersecurity: Where we Are; What more can be done? A call for auditors to lean in. Baruch College 18th Annual Financial Reporting Conference. Public Company Accounting Oversight Board (2019). https://pcaobus.org/news-events/speeches/speech-detail/cybersecurity-where-we-are-what-more-can-be-done-a-call-for-auditors-to-lean-in_700#_ednref26. Accessed 15 Aug 2022
31. Henseler, J., Hubona, G.S., Ray, P.A.: Using PLS path modeling in new technology research: updated guidelines. Ind. Manag. Data Syst. **116**(1), 1–19 (2016)
32. Hillson, D. Murray-Webster, R.: Managing risk attitude using emotional literacy. In: PMI® Global Congress 2006—EMEA, Madrid, Spain. Project Management Institute, Newtown Square (2006)
33. Hindson, A.: Risk appetite & tolerance guidance paper. The Institute of Risk Management (2013)
34. Hopstaken, J., Linden, D., Bakker, A., Kompier, M.: A multifaceted investigation of the link between mental fatigue and task disengagement. Psychophysiology **52**(3), 305–315 (2015)
35. International Organization of Securities Commissions (IOSCO): Cyber Security in Securities Markets – An International Perspective Report on IOSCO's cyber risk coordination efforts (2016)
36. Keinan, R., Bereby-Meyer, Y.: "Leaving it to chance"—Passive risk taking in everyday life. Judgm. Decis. Mak. **7**(6), 705–715 (2012)
37. Knechel, W.R.: The future of assurance in capital markets: reclaiming the economic imperative of the auditing profession. Account. Horiz. **35**(1), 133–151 (2021)
38. Kumar, K., Bakhshi, A.: The five factor model of personality: is there any relationship? Humanities Soc. Sci. J. **5**(1), 25–34 (2010)
39. Lance, C.E., Butts, M.M., Michels, L.C.: What did they really say? Organ. Res. Methods **9**(2), 202–220 (2006)
40. Harris, D. (ed.): EPCE 2013. LNCS (LNAI), vol. 8020. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39354-9
41. Li, H., No, W.G., Boritz, J.E.: Are external auditors concerned about cyber incidents? Evidence from audit fees. Audit.: J. Pract. Theory **39** (1), 151–171 (2020)
42. Linden, D., Keijsers, G., Eling, P., Schaijk, R.: Work stress and attentional difficulties: An initial study on burnout and cognitive failures. Work Stress. **19**(1), 23–36 (2005)
43. Mathauer, I., Imhoff, I.: Health worker motivation in Africa: the role of non-financial incentives and human resource management tools. Hum. Res. Health **4**, 1–17 (2006)
44. McDaniel, L.S.: The effects of time pressure and audit program structure on audit performance. J. Account. Res. **28**(2), 267–285 (1990)
45. National Institute of Standards and Technology (NIST): Guide for conducting risk assessments. NIST Special Publication 800–30 Revision 1 (2012)
46. National Internet Emergency Center: China's network security report in the first half year of 2021 (2021). https://www.cert.org.cn/publish/main/46/index.html. Accessed 15 Aug 2022
47. Neuman, G.A., Wagner, S.H., Christiansen, N.D.: The relationship between work-team personality composition and the job performance of teams. Group Org. Manage. **24**(1), 28–45 (1999)
48. Nolder, C.J., Kadous, K.: Grounding the professional skepticism construct in mindset and attitude theory: A way forward. Acc. Organ. Soc. **67**, 1–14 (2018)
49. Pittman, J.A., Stein, S.E., Valentine, D.F.: Audit partners' risk tolerance and the impact on audit quality. SSRN Electr. J. (2019)
50. Possible Questionnaire Format for Administering the 50-Item Set of IPIP Big-Five Factor Markers. International Personality Item Pool (2019). https://ipip.ori.org/new_ipip-50-item-scale.htm. Accessed 15 Aug 2022

51. Public Company Accounting Oversight Board (PCAOB): Other information in documents containing audited financial statements. Auditing Standards (AS) 2710 (2009). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2710. Accessed 15 Aug 2022
52. Public Company Accounting Oversight Board (PCAOB): Identifying and assessing risks of material misstatement. Auditing Standards (AS) 2110 (2010). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2110. Accessed 15 Aug 2022
53. Public Company Accounting Oversight Board (PCAOB): Standing Advisory Group Meeting: Cybersecurity (2014)
54. Reinartz, W.J., Haenlein, M., Henseler, J.: An empirical comparison of the efficacy of covariance-based and variance-based SEM. Int. J. Res. Mark. **26**(4), 332–344 (2009)
55. Rigdon, E.E.: Choosing PLS path modeling as analytical method in European management research: a realist perspective. Eur. Manag. J. **34**(6), 598–605 (2016)
56. Robbins, S.P., Judge, T.A.: Essential Organizational Behavior. Pearson Education Inc, Upper Saddle River (2008)
57. Rosati, P., Gogolin, F., Lynn, T.: Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. Int. J. Account. **54**(03), 1950013 (2019)
58. Rustiarini, N.: Pengaruh karakteristik auditor, opini audit, audit tenure, pergantian auditor pada audit delay. Jurnal Ilmiah Akuntansi dan Humanika, **2**(2) (2013)
59. Samagaio, A., Felício, T.: The influence of the auditor's personality in audit quality. J. Bus. Res. **141**, 794–807 (2022)
60. Sarstedt, M., Diamantopoulos, A., Salzberger, T., Baumgartner, P.: Selecting single items to measure doubly-concrete constructs: a cautionary tale. J. Bus. Res. **69**(8), 3159–3167 (2016)
61. Securities and Exchange Commission (SEC): Cybersecurity Roundtable (2014). https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml. Accessed 15 Aug 2022
62. Securities and Exchange Commission (SEC): Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018). https://www.sec.gov/rules/interp/2018/33-10459.pdf. Accessed 15 Aug 2022
63. Smith, K.J., Davy, J.A., Everly, G.S.: An assessment of the contribution of stress arousal to the beyond the role stress model. Adv. Acc. Behav. Res. **10**, 127–158 (2007)
64. Stoel, D., Havelka, D., Merhout, J.: An analysis of attributes that impact information technology audit quality: a study of IT and financial audit practitioners. Int. J. Account. Inf. Syst. **13**, 60–69 (2012)
65. Sawan, N., Alsaqqa, I.: Audit firm size and quality: does audit firm size influence audit quality in the Libyan oil industry?. Afr. J. Bus. Manage. **7**(3) (2013)
66. The Center for Audit Quality (CAQ): Cybersecurity risk management oversight: A tool for board members (2018). https://www.thecaq.org/wp-content/uploads/2019/03/caq_cybersecurity_risk_management_oversight_tool_2018-04.pdf. Accessed 15 Aug 2022
67. Trisnaningsih, S.: Independensi auditor dan komitmen organisasi sebagai mediasi pengaruh pemahaman good governance, gaya kepemimpinan dan budaya organisasi terhadap kinerja auditor. Jurnal Simposium Akuntasi Nasional, UNHAS Makasar (2007)
68. van der Kaap-Deeder, J., Brenning, K., Neyrinck, B.: Emotion regulation and borderline personality features: the mediating role of basic psychological need frustration. Personality Individ. Differ. **168**, 110365 (2021)
69. Xue, Z.: China CFO insights - Seven hidden costs of a cyberattack (2017). https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/finance/deloitte-cn-cfo-insights-seven-hidden-costs-cyberattack-zh-170403.pdf. Accessed 15 Aug 2022
70. Zhou, H., Lv, C.: Does accounting firm size change investors' perception of audit quality? Chin. Account. Financ. Rev. **9**(3) (2007)