RGSA – Revista de Gestão Social e Ambiental
ISSN: 1981-982X
Data de submissão: 12/23/2023
Data de aceite: 03/11/2024
DOI: https://doi.org/10.24857/rgsa.v18n6-008
Organização: Comitê Científico Interinstitucional
Editor Chefe: Christian Luiz da Silva
Avaliação: Double Blind Review pelo SEER/OJS

THE ROLE OF INTERNAL AUDITORS CHARACTERISTICS IN CYBERSECURITY RISK ASSESSMENT IN FINANCIAL-BASED BUSINESS ORGANISATIONS: A CONCEPTUAL REVIEW

Alih Usman[1]
Ayoib Che-Ahmad[2]
Salau Olarinoye Abdulmalik[3]

ABSTRACT

Purpose: This paper aims to establish a theoretical framework that will enhance the examination of the role of internal auditors in cybersecurity risk assessment in financial-based business organizations. Financial-based business organizations are institutions or companies that render financial services to public and private stakeholders in an economy. It is a powerful sector in the economy of every country. This drive poses a lot of challenges to organizations. Hence, business organizations strategically devised a means to safeguard the integrity, confidentiality, and availability of information. Also, innovation poses many risks and threats to the internal audit function in an organization.

Theoretical Framework/Findings: Using the competency and planned behaviour theories (McClelland 1973 and Ajzen,1991), this study disclosed that the task performance of cybersecurity risk assessment by the internal auditor is influenced by the required internal auditor's characteristics of professional ethics of integrity and objectivity, personality traits, professional skills competency professional knowledge competency and deterrence and rewards to advise the management on the implications of cyber security risk on business organisations for monitoring and mitigations.

Methodology: A literature review approach is adopted to highlight the role of internal auditors in cyber security risk assessment in financial–based business organizations.

Research Limitation/Implication: This conceptual paper has consequences for the practice of internal auditing. This approach is helpful to academic scholars in testing it out in the real world. This model is helpful to practitioners when evaluating the function of IAs in the cybersecurity risk assessment context.

Originality/Values: Earlier auditing-related studies haven't addressed this problem. This study makes an effort to close such a gap and investigate the subject of the internal auditor's characteristics and cyber security risk assessment among financial-based organizations.

Keywords: Cyber Security, Risk Assessment, Internal Auditors, Financial Organizations.

O PAPEL DAS CARACTERÍSTICAS DOS AUDITORES INTERNOS NA AVALIAÇÃO DOS RISCOS DE CIBERSEGURANÇA EM ORGANIZAÇÕES EMPRESARIAIS DE BASE FINANCEIRA: UMA REVISÃO CONCEPTUAL

RESUMO

Objetivo: Este documento visa estabelecer um quadro teórico que melhorará o exame do papel dos auditores internos na avaliação de riscos de cibersegurança em organizações empresariais de base financeira. Organizações de negócios com base financeira são instituições ou empresas que prestam serviços financeiros a partes interessadas públicas e privadas em uma economia. É um setor poderoso na economia de todos os países. Essa

[1] College of Business, Tunku Puteri Intan Safinaz, School of Accountancy, Universiti Utara Malaysia. Kogi State University. Nigeria. E-mail: usman_alih@uum.edu.my
[2] College of Business, Tunku Puteri Intan Safinaz, School of Accountancy, University Utara Malaysia. Malaysia. E-mail: ayoib@uum.edu.my
[3] College of Business, Tunku Puteri Intan Safinaz, School of Accountancy, University Utara Malaysia. Malaysia. E-mail: salau@uum.edu.my

unidade representa muitos desafios para as organizações. Assim, as organizações empresariais desenvolveram estrategicamente um meio de proteger a integridade, a confidencialidade e a disponibilidade das informações. Além disso, a inovação representa muitos riscos e ameaças para a função de auditoria interna de uma organização.

Estrutura Teórica/Descobertas: Usando as teorias de competência e comportamento planejado (McClelland 1973 e Ajzen, 1991), este estudo revelou que o desempenho de tarefas de avaliação de riscos de segurança cibernética pelo auditor interno é influenciado pelas características do auditor interno necessárias de ética profissional de integridade e objetividade, traços de personalidade, competência de habilidades profissionais, competência de conhecimento profissional e dissuasão e recompensas para aconselhar a gestão sobre as implicações do risco de segurança cibernética em organizações empresariais para monitoramento e mitigação.

Metodologia: É adotada uma abordagem de revisão de literatura para destacar o papel dos auditores internos na avaliação de riscos de segurança cibernética em organizações de negócios de base financeira.

Limitação/Implicação da Pesquisa: Este documento conceitual tem consequências para a prática de auditoria interna. Essa abordagem é útil para acadêmicos em testá-la no mundo real. Este modelo é útil para os profissionais ao avaliar a função das AI no contexto da avaliação de riscos de cibersegurança.

Originalidade/valores: estudos anteriores relacionados à auditoria não abordaram esse problema. Este estudo faz um esforço para colmatar essa lacuna e investigar o tema das características do auditor interno e da avaliação dos riscos de cibersegurança entre organizações de base financeira.

Palavras-chave: Segurança Cibernética, Avaliação de Riscos, Auditores Internos, Organizações Financeiras.

EL PAPEL DE LOS AUDITORES INTERNOS EN LA EVALUACIÓN DE RIESGOS DE CIBERSEGURIDAD EN ORGANIZACIONES EMPRESARIALES DE BASE FINANCIERA: UNA REVISIÓN CONCEPTUAL

RESUMEN

Objetivo: El presente trabajo tiene como objetivo establecer un marco teórico que permita mejorar el examen del papel de los auditores internos en la evaluación del riesgo de ciberseguridad en las organizaciones empresariales de base financiera. Las organizaciones empresariales de base financiera son instituciones o empresas que prestan servicios financieros a interesados públicos y privados en una economía. Es un sector poderoso en la economía de todos los países. Este impulso plantea muchos desafíos a las organizaciones. Por lo tanto, las organizaciones empresariales idearon estratégicamente un medio para salvaguardar la integridad, confidencialidad y disponibilidad de la información. Además, la innovación plantea muchos riesgos y amenazas a la función de auditoría interna de una organización.

Marco teórico/Hallazgos: Utilizando las teorías de competencia y comportamiento planificado (McClelland 1973 y Ajzen, 1991), este estudio reveló que el desempeño de la tarea de evaluación de riesgos de ciberseguridad por parte del auditor interno está influenciado por las características requeridas del auditor interno de ética profesional de integridad y objetividad, rasgos de personalidad, habilidades profesionales, competencia, conocimiento profesional, competencia y disuasión y recompensas para asesorar a la administración sobre las implicaciones del riesgo de ciberseguridad en las organizaciones empresariales para el seguimiento y las mitigaciones.

Metodología: Se adopta un enfoque de revisión de la literatura para destacar el papel de los auditores internos en la evaluación de riesgos de ciberseguridad en las organizaciones empresariales de base financiera.

Limitación/Implicación de la Investigación: Este documento conceptual tiene consecuencias para la práctica de la auditoría interna. Este enfoque es útil a los académicos para probarlo en el mundo real. Este modelo es útil para los profesionales a la hora de evaluar la función de las EI en el contexto de la evaluación de riesgos de ciberseguridad.

Originalidad/Valores: Estudios anteriores relacionados con la auditoría no han abordado este problema. El presente estudio pretende cerrar dicha brecha e investigar el tema de las características del auditor interno y la evaluación de riesgos de ciberseguridad entre las organizaciones financieras.

Palabras clave: Ciberseguridad, Evaluación de Riesgos, Auditores Internos, Organizaciones Financieras.

RGSA adota a Licença de Atribuição CC BY do Creative Commons (https://creativecommons.org/licenses/by/4.0/).

1 INTRODUCTION

The concept of cyber security risk assessment (CSRA) entails all the procedures, policies, safeguards, and internal control measures, put in place by business organizations for the identification, classifying, evaluation, and reporting of cybersecurity risks incidence to the board for the safety of the integrity, confidentiality, and availability of information technology from the attacks of unauthorized internal and external malicious forces and criminals (Ajiji, 2019; NIST, 2018; Steinbart & Raschke, 2018). Cybersecurity is set up by business organizations to checkmate the attack on public and private critical infrastructures such as identity theft, malware, ransomware and email phishing to ensure risk prevention, mitigation, and monitoring to safeguard critical infrastructures for optimum productivity (IIA, 2017a; Pricewaterhouse Coopers, 2017 & Usman et al.2021). This is because, traditional means of internal control measures are not effective and efficient in safeguarding information technology in a financial-based business organization globally (Ajiji, 2019; Lois et al., 2021).

Extant studies have focused on cybersecurity awareness and information security investment initiatives in the advanced and emerging economy (Lamboglia et al., 2020; Shamsuddin, 2018; Tsohou, 2018; Gordon et al., 2018b; Yang et al., 2020). Likewise, the association between the audit committee and cybersecurity breaches has been studied in the underdeveloped economy (Daud et al., 2018; Ojeka et al., 2017c; Pundmann et al., 2017). Other studies have examined the effects of cybersecurity incidents on firms and their reputations (Catota et al., 2018; Minto-Coy & Henlin, 2018; Ndeda et al., 2019; Osho & Onoja, 2015a) and the relationship between security programs and optimal investment in security (Euphemia, et al., & Onyekachi, 2019; Gordon et al., 2015, 2018b; Kisekka, 2018; Steinbart & Raschke, 2018). Babo, S.Alon, I.& Paltrinieri, A (2020) fraudulent acts of corrupt practices are multidimensional areas which have attracted scholars' attention from different fields and disciplines to examine. Literature has also examined the legislating, determining and ways of kinetic means of combating crimes such as cybersecurity risk and other business organisation risks globally (B et al 2020).

Despite the extensive studies on cybersecurity, few have offered insights into the internal auditor's role and characterization both conceptually and theoretically (Betti & Sarens, 2020a; Erin et al., 2020; Haapamäki & Sihvonen, 2019a, 2019b; Islam et al., 2018a; Kure & Islam, 2019; Shamsuddin, 2018a; Shamsudin et al., 2019; Steinbart & Raschke, 2018). To the researcher, there are fewer theoretical emphases on cybersecurity risk assessment, internal auditor's attributes, and cybersecurity risk assessment. Specifically, (Betti & Safinancial–basedaapamäki & Sihvonen, 2019a); (Islam et al., 2018); and (Steinbart & Raschke, 2018) called for further theoretical and empirical examination of cybersecurity risk management in business organizations. This paper seeks to fill such a gap in extant studies by focusing on the role of internal attributes in cybersecurity risk assessment among financial-based business organisations. The objectives of the paper are conceptualized if (1) internal auditors' professional ethics enhance the cybersecurity risk assessment in a financial-based business organization (2) the internal auditor's personality trait impact cybersecurity risk assessment in financial–based business organization (3) the internal auditor's skills competency enhances task performance cybersecurity risk assessment in a financial-based business organization (4) the internal auditors knowledge competency influence task performance cybersecurity risk assessment in financial-based business organization and (5) to determines if internal auditors deterrence and rewards enhance task performance cybersecurity risk assessment in financial-based organisations. The plausible reason for the global increase in cybercrime is individuals who lack cybersecurity awareness and a poor management attitude toward cybersecurity risk (Slapničar et al., 2022; Vuko et al., 2021; Zwilling et al., 2020). Also, the absence of strict corporate governance control measures with a risk assurance framework makes the identification, detection, and monitoring of risk and control more difficult in thE financial service environment (Erin et al., 2020; Ogunjobi, 2020; Ojeka et al., 2017; Marei et al 2023).

This is because employees of an organization such as a financial-based business organization require certain attributes to embark on task performance cybersecurity risk assessment in business organizations globally. To actualize the stated objectives of the study, the remaining part of the paper is therefore organized as follows: Section 2 provides the theoretical framework. Section 3 discusses methodology, Section 4 provides results and discussion. Section 5 concludes the paper with frontier for further investigation.

2 THEORETICAL FRAMEWORK

The importance of business organizations and professional bodies in ensuring critical infrastructure security has attracted much advocacy. Consequently, the quest for factors responsible for information technology security is of great significance. Therefore, the present study framework is built on the competency and reason action/planned behaviours theories which are liked with internal auditor's characterization and cybersecurity risk assessment with mediating role of cybersecurity threats awareness. These theories are seen to have constituted the basic linkages conceptually and theoretically in terms of internal auditors' competencies in task performance cybersecurity risk assessment. The competency theories are associated with internal auditors' attributes because, the theories indicate that human intellect is an indicator of performance in an organization (McClelland, 1973; Muse et al., 2018; Sunyoto, 2020).In addition, the choice of the underpinned theories is based on the theories' concept of capability in the area of skills, knowledge, professional ethics of integrity and objectivity, skills, knowledge and other proficiency characterisations as personality traits and deterrence and rewards that are the required characterisation of a professional such as the internal auditors in carrying out efficient and effective obligation in the cybersecurity risk assessment in an organization.

McClelland established the competency theory as a predictor of human performance (1973). It is used as a human resource tool for appraisal, selection, training and development, and succession planning since it describes the precise knowledge, abilities, and traits required to effectively perform an organisation's function (Muse et al., 2018; Novikova, 2013). The competency approach, as defined by (McClelland, 1973; Muse et al., 2018; Sunyoto, 2020), is that the theory is perfect for identifying individual potentials for efficient performance, which in turn affects business organization outcomes.

Internal auditors will not be able to stay one step ahead of cybercriminals unless they have the necessary characterisations and competencies, as stated in this study on how cybercriminals professionally interpret acts. The competency theory was found to be the most appropriate for the IA characterization as it is a link and related to the variables apart from the deterrence and rewards construct in the study as an organisation's management determines the level of information to utilize when describing the competencies that will be included in the intended competency model (Muse et al., 2018; Slapničar et al., 2022). A competency model

is a tool that can be used to assess the degree of competence of employees' task performance such as cybersecurity risk assessment in business organisations.

The competency model classically includes a list of competencies and behavioural indicators that make it comes alive regarding what it looks like in the context of an organisation. From the empirical studies, (Jena & Sahoo, 2014), conducted a study on the improved managerial performance on entrepreneurial and leadership competencies. Fifteen (15) independent variables were used in the study, out of which only three factors extracted (business knowledge, the dimension of leadership and spirit of competitiveness) were found to be significant concerning the task performance of the organisations.

As a contribution to the literature and practical studies, this study claimed that the five internal auditors' characterisations of competencies are critical for outstanding managerial task performance in cybersecurity risk assessment. Glass & Metternich, (2020) also research auditor's competency modelling in extension education: combining an academic extension education model with a human resource management extension model. Scheer adopted seven (7) distinct capabilities for the human resource management approach. In addition, the research revealed potential educational opportunities for both credit and non-credit instruction.

Competencies and the attributes of the IA in the financial industry required and proposed for the prevention of cybersecurity risk in this study include (Professional Ethics, Personality Traits, Skills, Knowledge, Deterrence, and Rewards). Internal Auditors need competencies and tools to accomplish their task performance, especially when it comes to cybersecurity risk assessments. A competency model, according to Bolt-lee & Foster, (2014), is a documented description of the competencies required for totally successful or excellent task performance in a job category, work team, department, division, or organization. Boyatzis, (2008) and Fallis, (2007) described competencies as a person's cognitive (knowledge and skills), affective (attitudes, ethics, and values), behavioural, and motivational characteristics and dispositions, such as (personality traits and values) that enhance task performance such as cybersecurity risk assessment.

Individual talents and human resource functions are also aligned with organizational strategies using the competency model (Özçelik & Ferman, 2006). This is appropriate for financial service business organizations, such as banks, with the primary goal of identifying, mitigating, evaluating, assessing, preventing and monitoring cybercrime and establishing risk assurance stewardship. As a result, competency theory provides a better understanding of the aspects that contribute to cybercrime by emphasizing competencies and attributes such as

(Professional Ethics, Personality Traits, Skills, Knowledge, Deterrence, and Rewards). Internal auditors can apply the competency model in a variety of ways, including cybersecurity risk assessment.

Similarly, the theory of planned action behaviour emphasizes that humans are rational thinker that thinks about the cost and benefits of an action before embarking on any action in an organization (Sheppard et al., 1988; Ajzen, 1991). Since 1918, the notion of reasoned and planned action theory has been employed to explain people's behaviour based on their attitudes (Sheppard et al., 1988). Expectancy value theories in social psychology are the source of this hypothesis. The idea of reasoned action was intended to explain essentially any human behaviour (Ajzen, 1991; Muse et al., 2018; Odumesi, 2014b). Individuals are reasonable, according to the principle of reasoned and planned action theory. They are expected to make systematic use of the information at their disposal to execute the necessary, reliable, and relevant actions. Individuals, in essence, examine the consequences of their behaviours before deciding whether or not to engage in a specific behavioural setting (Aljohani & Elfadil, 2020; Muse et al., 2018; Zhang, 2018).

The theory of reasoned/planned action asserts that intention is the most accurate predictor of behaviour when making logical judgments (Ihekwoaba et al., 1971; Kassem & Turksen, 2021; Odumesi, 2014). Furthermore, the theory of reasoned action has revealed that behavioural intentions, which are a combination of attitudes toward the performance of the behaviour and subjective norms, are the most important determining factor of an individual's behaviour.

However, study such as Ajzen, (1991) limits the notion of reasoned action. In the same vein, Sheppard et al., (1988); and Sherwood, (2020) support this by stating that to anticipate specific behaviour, intention and attitude must agree on a path of action. Because attitude and subjective norms have a substantial impact on the behaviour of individuals such as the Internal Auditor deterrence and rewards in the cybersecurity risk assessment of an organisation. Therefore, the theory of reasoned action may be pertinent to the current study as it has a link with IA deterrence and the rewards construct of an employee in an organisation.

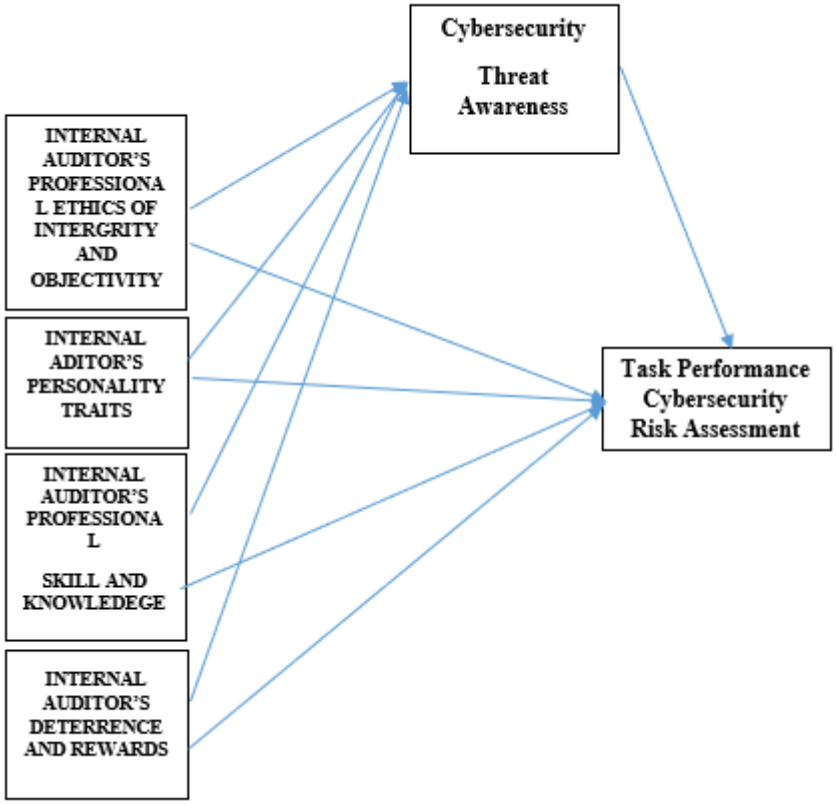
This theory describes how people make decisions based on rational decision-making that has been assumed in models of criminal behaviour (e.g., situational crime prevention, routine activity theory). To examine this assumption, Richardson, & Vasvari, (2008) Cho et al., (2012); Ife et al., (2021); and Purpura, (2013) established the rational choice theory. This theory explains why and how offenders make rational decisions to commit a crime, as well as

what can prevent them from doing so, by looking at different criminal events in terms of (perceived) opportunity, costs, and rewards. This theory holds for physical crime, but it may hold even truer for cybercrime. That is to say, there is a significant logical component. A user may come upon a defect on a website and, rather than reporting it to the site's owners, be enticed to investigate what may be accomplished by exploiting the bug, such as gaining access to accounts whose credentials had just been disclosed in plaintext. Even the most experienced and intelligent players, such as hackers, may not always be aware of the criminality of some of their behaviours in cyberspace, making it difficult to distinguish between what is legal and what is illegal. Therefore, the outcome of the act determined the positions of the actors. Similarly, the benefit accrued to the honest employee in the form of the reward of financial and -non-financial enhances the task performance of an employee in an organisation (Ihekwoaba et al., 1971; Ndungu, 2017; Qaiser Danish et al., 2015). Consequently, this study is suggesting that the theory is related to the IA deterrence and reward characterisation and task performance cybersecurity risk assessment. Hence their choice for this study is depicted in Figure 1.

The framework is consistent with (Islam et al., 2018a; Vuko et al., 2022; Lois et al., (2021) and Salleh & Aziz, 2014) with basic modification in the introduction of deterrence and rewards, professional ethics of integrity and objectivity, and the mediating role of cybersecurity threats awareness constructs while concentrating on task performance cybersecurity risk assessment in the financial based business organisations.

Figure 1

Theoretical Framework of the study



Source: Adopted from (McClelland, (1973); Ajzen, (1991); Islam et al., 2018a; Vuko et al., 2022; Lois et al., (2021) and Salleh & Aziz, 2014)

2.1 INTERNAL AUDITORS' CHARACTERISTICS

An internal auditor is an independent individual, engaged in the professional task of an organization to show a true and fair view of the business organization (IIA, 2020; Pricewaterhouse Coopers, 2017 & Elaigwu et al. 2020). Studies reveal that for an internal auditor to embark on professional responsibilities, it required certain characteristics or attributes of competencies which may influence task performance (AICPA, 2018; IIA, 2017a; Islam et al., 2018b). These capabilities and proficiencies proposed are the professional ethics of integrity and objectivity, personality traits, professional skills and knowledge competencies, and deterrence and rewards.

2.2 INTERNAL AUDITORS PROFESSIONAL ETHICS OF INTEGRITY AND OBJECTIVITY

Professional ethics of integrity and objectivity entail the objectives and beliefs that create behaviour and provide a basis for decision-making (Aldasoro et al., 2020; Bondarenko & Kryzhanovska, 2020). In a profession such as auditing and accounting, professional ethics are the standards for actions that are prepared by experts and professional bodies. They established frameworks for evaluating behaviours (IIA, 2017b). Auditing is a profession rooted in professional ethics and the audit role is based on such ethics and values. Basic ethics and value in the internal audit profession include independence and objectivity, honesty, human dignity, and social justice (Hamshari, 2021; Zwilling et al., 2022). Therefore, the values are generally shared within the business environment globally and are a reflection of the human and spiritual approach to the auditing profession (Steinbart & Raschke, 2018).

However, the professional ethics of integrity and objectivity in the cybersecurity risk assessment are affected by cultural, socioeconomic and religious conditions which are dominant in business organizations (Pasculli, 2020; Şahin et al., 2009) This makes it essential to identify such ethics respectively in each organisation. Extant studies reveal that the professional ethics of the internal auditors enhance cooperate task performance for goal achievement (AICPA, 2017; IIA, 2017a; Haapamäki & Sihvonen, 2019; Steinbart et al., 2015; Steinbart & Raschke, 2018)). The professional ethics code which is the module operandi clarifies the internal auditing profession and practices, the quality of professional care, and professional norms respectively (Dzikrullah et al., 2020). Advances in technology and the expansion of the IA role have sparked complex ethical confusion for the IA (Radoilska & Ceva, 2021; Tehranineshat et al., 2020). Such a dilemma if not adequately managed in an organisation, would negatively affect the ability of a novice IA to make a comprehensive assessment of the cybersecurity risk independently and objectively.

Consequent to the errors emanating from the ethics among the auditors in their responsibilities, the promotion of ethics has become more critical in auditing awareness. Studies indicate that the acquisition and internalization of ethics may positively affect IA in task performance cybersecurity risk assessment in an organization (Poorchangizi et al., 2019; Sunyoto, 2020 & Alih et al.2019). The components of professional ethics of an IA could be seen from the perspective of the nature of the ethics and approaches, ethical behaviours at the workplace, ethics in the business organisation, corporate governance, business and

environmental ethics, working in public interest whistleblowing and IT system fraud and money laundry ethics standards (Luthan et al., 2019; Tehranineshat et al., 2020).

Meanwhile, a study by Bidabad & Sherafati (2016) and Tehranineshat et al. (2020) states that the professional ethics of professionals in a workplace have a positive impact relating to task performance. However, these studies were conducted in the context of the health sector in a developed economy's sectors as focal points. Similarly, studies have shown that employees with professional ethics positively and significantly influence the management and mitigation of risk and internal control of financial institution operation assets (Bondarenko & Kryzhanovska, 2020; Idid & Arandas, 2016; Nurnaluri et al., 2021; Watkinson, 2013). However, these variables have not been tested in the context of corporate governance mechanisms with an insight into task performance cybersecurity risk assessment. Additionally, another significant factor of internal auditors' characterization in organization task performance cybersecurity risk assessment is a personality trait (Soto & Jackson, 2013; Soto & John, 2009).

2.3 INTERNAL AUDITOR'S PERSONALITY TRAITS

To appreciate the role of internal auditors in the task performance cybersecurity risk assessment in companies such as financial institutions, it is significant to acknowledge that individual varies. Therefore, it is likely that one behaviour of an individual can influence others in society and business organisations (Kuijck & Paresi, 2020; Mooradian et al., 2006). However, it could be pertinent to state that differences in characters can lead many people to perpetrate a crime against humanity, the business organization environment and the IT system and internet and other government and private critical infrastructure. Institutions such as banking companies cannot be left out of attacks (Makeri, 2017). Conceptually, personality is defined as a pattern of thought, emotion, and individual characters that are considered stable sometimes, which are psychological and can serve as a yardstick for individual actions (Baron & Kenny, 1986; Kuijck & Paresi, 2020).

Extant studies have stated that personality features are mostly stable and patient, have structure, and are dynamic in individuals, and the absence of great situational impact can play a fundamental role in individual and organizational characterizations (Products et al., 2018; Yunus et al., 2018). Specifically, personality has been used to assess and identify the various aspect of risk related to IT systems and cybersecurity risks and threats in an organization (Czerniawska & Szydło, 2021). Studies have differentiated between various personalities of

Information Technology professionals but other research in these areas on cybersecurity professionals appeared so scanty (Tedeholm et al., 2021).

Extant studies state that different personality trait dimensions such as openness, conscientiousness, Extraversion, Agreeableness, and Neuroticism (Albawwat & Al Frijat, 2021; Carlton & Levy, 2017; Macnish & van der Ham, 2020; Pérez-sánchez et al., 2021; Sohrabi Safa et al., 2016; Thompson, 2018) impact positively in the mitigation of cybersecurity risk and threats among corporate organisations in information technology. However, these areas split further into trait facets at the second level (Czerniawska & Szydło, 2021; Vuko & Slapnicar, 2021).

Openness to experience explained the length, breadth, originality and nature of one's skills with those that may score high in the domain as described as original, curious and imaginative. Openness to experience involves facets such as Adventurousness, Artistic, Interests, Emotionality, Intellect, Imagination, and Liberalism (Albawwat, et al, 2021; Czerniawska & Szydło, 2021; Deyoung et al., 2014; Kuijck & Paresi, 2020; Vural & Eskici, 2020). In a specific term, conscientiousness entails impulse management that can impact risk control and aimed oriented character which may involve gratification, taking the necessary procedures and planning, organising, and as well, prioritising task performance in an organisation (Yunus et al., 2018). It also includes facets such as Achievement Striving, Cautiousness, Dutifulness with orderliness and discipline and self-discipline (Mylavarapy, 2016; Novikova, 2013; Parks-Leduc et al., 2015b).

Extraversion, on the other hand, signifies a strong methodology to life and those scoring high in the domain and self-soundness. It equally includes facets such as Activity level, Assertiveness, Cheerfulness, Excitement Seeking, and Friendliness (Tedeholm et al., 2021). Agreeableness is related to prosaically and community training targeted at others with personnel with high scores in the areas seen as beneficial, and friendly (Kuijck & Paresi, 2020). The facet in this aspect of the big five includes Altruism, Cooperation, Modesty, Sympathy, Morality and honesty (Kuijck & Paresi, 2020; Moustafa et al., 2021; Soto & John, 2009). Neuroticism in the final note implies and involves tension, vulnerability, and irritability along the lines of stress with those with high scores in the area that have been described as hostile and less able to manage impulses. The facet includes Anger, Anxiety, Depression, Immoderation, Self-Consciousness, and Vulnerability (Kuijck & Paresi, 2020; Soto & John, 2009; Yunus et al., 2018). Meanwhile, this study conceptualized honesty, pity, irritability, cautiousness, anxiety and intellectualism.

Honesty: Extant studies on uniform personnel scores greater than the average numbers in the areas Agreeable (Garbarino et al., 2012, 2013; Macnish & van der Ham, 2020). This signifies that cybersecurity professionals such as the IA may score averagely different on selected facets in the area due to their resemblance to uniform workers of policing. The honesty facet from the dimension of Agreeableness may be synthesized into two broad sectors: Interpersonal and propensity to honesty. Interpersonal honesty is the willingness of a party to be vulnerable to the actions of other parties of the expectation that significant actions will be taken by the other party in response to honesty, this is irrespective of the controllability ability of other party actions (Ferreira-Oliveira, 2017). This category of honesty is the term to be appreciated as situational and relates to specific persons such as executives or their subordinates.

Therefore, the propensity to honesty on the other hand is described as an enduring predisposition that is neither focused on others nor dependent on specific contexts, and that may be associated with life experience but also with temperament, and thereby to genetics and physiological structure. Therefore, for this study, the personality of the IA in the cybersecurity risk assessment would be put into consideration to ascertain the propensity to honesty since the trait is significant in the IA characterization and task performance cybersecurity risk assessment in an organization.

Johnson & Mislin, (2011) enumerated that individuals such as the IA who score high on the facet of honesty may assume to be generally fair in their dealing with cybersecurity with honesty and good intentions. Whereas internal auditors who scored low on this facet are considered to be selfish and potentially dangerous in the IT system environment (Koziarski & Lee, 2019; Santucci, 2018b). Meanwhile, cybersecurity assessors are expected to be thinking contently of new ways to enhance ways of having a low honesty on people as malicious actors in the business ecosystem could be a great threat. Therefore, IA is not to be sympathetic in their facet of cybersecurity risk assessment in an organization.

PITTY: From the Agreeableness facet, pity would be chosen in addition to honesty for examination due to its resemblance between cybersecurity professionals and uniform service forces such as police officers (Garbarino et al., 2012, 2013; Johnson & Mislin, 2011). This is because IA professional who tends to score high grades on the Likert scale on the pity facet are seen to be “tender-hearted and compassionate. They feel the pain of others vicariously and are easily influenced by pity”.

In another development, cybersecurity management professionals with low scores are referred to understand: not to be affected strongly by human suffering. They place themselves on making fundamental judgments based on reason. They are, however, more worried with honesty and justice and mercy". These analyses of pity categorized the facet into tender-mindedness and tough-mindedness. Tough-mindedness entails the process of making decisions based on fundamental logic, facet, and data as opposed to feelings. Tender-mindedness, however, typically relied on making decisions based on emotion and illogical perspectives (Buckner et al., 2012; Tedeholm et al., 2021). Therefore, cybersecurity professionals such as the IA are required to base their task performance on facets and data to make honest and accurate judgments and decisions making. This involves careful planning and assessment which are necessary for cybersecurity vulnerability outcomes. In a related development, professional skills competency is another factor that influences internal auditors' task performance

2.4 INTERNAL AUDITORS PROFESSIONAL SKILLS COMPETENCY

Skills are conceptually seen as a feature of an employee as internal auditor that is associated with competencies in the duties of risk assurance knowledge and capacity in those areas which relate to task performance in cybersecurity risk assessment in an organisation's business environment (Betti & Sarens, 2020; Suzuki, M., Ando, N., & Nishikawa, H. 2022; Carlton et al., 2019; Chambers & Mcdonald, 2013; IIA, 2017a). Therefore, the skills and capacity of the IA refer to whether the employees or individuals possess the required skills and wisdom in skills to discharge their duties diligently. The capacity aspect of the features entails the ability of the IA to translate the skills into task performance cybersecurity risk assessment (Alhazmi, 2015; Carlton et al., 2019; IFAC, 2011, 2015, & Yanita. et al 2023)). However, studies indicate that skills requirements for the internal auditors to actualize the task performance cybersecurity risk assessment could be intellectual skills, technical and operational skills, communication and interpersonal skills within the organization and business management skills (Carlton & Levy, 2017a; IFAC, 2011, 2015).

Internal auditor's skill in another way entails the exclusive skills that are developed purposely to gather proof for the primary aim of cyber risk identification, evaluation, and monitoring as well as preventing and mitigating crimes with corresponding responses unlike other areas of auditing that are meant for the aims of providing reasonable assurance which may be fairly taken with material respect. Zweighaft, 2017).

Therefore, cybersecurity risk assessment required an internal auditor who has the technical and intellectual skills to demonstrate the application of investigation and analytical skills associated with the area of audit records, gathering and evaluating proofs, assessing and interviewing all parties involves in cybersecurity risk incidences and serving as an expert in cyber-attacks cases (Agbo et al., 2020; Betti & Sarens, 2020b; Ferracane, 2019). However, the internal auditor is expected to have the exclusive skill to enable him to examine the proof, and vulnerability of the attacks on the organization from different ends that have comprehended the remote and immediate causes of the cybersecurity attacks (Gundu et al., 2019). Meanwhile, a study (Betti & Sarens, 2020b) on the understanding of the internal auditors in a digitalised business environment reports that the agility of the IA affects task performance in three perspectives, the scope, planning and the required digital knowledge increased space which will decrease the incidence of cybersecurity risk in business organisations, it also enhances the demand for IA consulting activities and leads to the modification of the working practices of a digitalised IA task performance (Betti & Sarens, 2020b).

2.5 INTERNAL AUDITORS' PROFESSIONAL KNOWLEDGE COMPETENCY

Studies document that an internal auditor needs fundamental auditing knowledge which must include: "Professional duties and practice administration, legal, court and disagreement settlement, strategic planning and preparation, intelligence and information gathering and filing (such as documents, interviews, technical and electronic and data) risk assessment, identification, expert and testimony (Digabriele, 2008; Zwilling, 2022; Zwilling et al., 2022).

Tsohou, (2018) concords with the submission that an IA is required to acquire a higher degree of competence, honesty, integrity, and professional qualifications to enhance task performance in an organization. Therefore, IA must be thoroughly trained and prove beyond a reasonable doubt, his competence by overcoming all relevant examination challenges to become relevant among the recognised auditing body. IIA, (2017a) stated that the competence requirement of an internal auditor's knowledge includes historical financial information audit at a greater level, information security at a higher level, and financial auditing and internal risk control at a higher-level knowledge.

The certification in the core areas of internal auditing function signified specialization of internal auditor knowledge including risk identification, evaluation, and monitoring coupled with legal knowledge, computer analysis, bankruptcy, insolvency and economic, financial cost

and reputational damages computation (Bruijn & Janssen, 2017; Islam et al., 2018a; Zweighaft, 2017; Zwilling et al., 2020). Therefore, this study looked at the fundamental knowledge such as technical, professional, educational or intellectual knowledge required for the assessment and mitigation of cybersecurity risks. The essence is that a mere effective auditor does not guarantee effective cybersecurity risk and threats detectives, assessment and monitoring (Carlton & Levy, 2017b; Garba et al., 2020; Shamsuddin, 2018a). Therefore, an internal cybersecurity auditor requires the professional to pose a fundamental spectrum of skills, knowledge and professional ethics on the statutory responsibilities of the task.

Studies have shown that as the state of business organisations expands in size and complexity, discovering cybersecurity risk needs professional auditing and accountants to be proactive with necessary characterizations in an increasing rate of professional skill, and knowledge competency. Some of the indices of professionalism include a thorough knowledge of the financial background, risk scheme, internal control strategies, psychology and criminologist skills, criminal and civil law knowledge, organization corporate governance and policies knowledge, computers and network proficiency skills, and IT communication skills (Ramasamy & Woan Ting, 2004; Rasool et al., 2017).

Meanwhile, this study suggested that IA's knowledge as a characterization of professionals in cybersecurity risk control is expected to encompass attributes for the designing of the audit procedures which are necessary to give adequate proof to reasonable assurance that cybersecurity is free from malicious attack. Similarly, (Sunyoto, 2020) examines the influence of IA's experience, professional commitment, and performance in financial companies, the study reveals that IA's level of experience and knowledge significantly influence IA's task performance. However, judging from (Thabet, 2016), this study assumed that IA professional knowledge associated with technical, academic training and business world knowledge with h problem-solving ability and other cognitive attributes impact positively task performance cybersecurity risk assessment.

2.6 INTERNAL AUDITORS' DETERRENCE AND REWARDS

Deterrence and rewards could be used as fundamental variables for the assessment and mitigation of cybersecurity risks in an organisation. The theory of deterrence is a comparative framework that evolved from the work of Hobbes, Beccaris and Benethan (D'Arcy & Herath, 2011; Herath & Rao, 2009b; Ihekwoaba et l., 1971; Products et al., 2018). However, the theory

has three main components which are: severity, certainty and celerity (Carlton et al., 2019; National Institute of Standards and Technology (NIST), 2020). Classical deterrence theory states that penalties must be seen to be severe, swift, and pure to deter crimes such as cybersecurity attacks (Eisenbach et al., 2020; Herath & Rao, 2009a; Koziarski & Lee, 2019). The theory assumed that the rational behaviour of the subject is involved in an interaction. The theory has been used in extant studies to avert inappropriate behaviours in the use of IT systems, such as computer mismanagement and security policy violations (Loh et al., 2019; Xu et al., 2019). The study also reports that the theory can equally be used to resolvpeople' aspects of information security control. Hence, this study conceptualized the facet as a useful tool of IAs for the internal control and mitigation of cybersecurity risk. The extant study states that IA with a better incentive in an organisation impacts positively on the internal control of cybersecurity risk assessment and mitigation (Lindsay, 2017; Ndungu, 2017; Yilmaz, 2019).

2.7 MEASURE OF IA'S CHARACTERISATIONS

While the IAs attributes and competencies measurement has been one of the most extensively studied areas in internal auditing literature (Haapamäki & Sihvonen, 2019a; Islam et al., 2018b; Vuko et al., 2021), competencies of IA are a verging field in business organization corporate governance research. Many factors that influence IAs' competencies and attributes are generically proven. However, cyber security risk control measures, (Betti & Sarens, 2020a; Vuko et al., 2021) can be assumed to have been capable of affecting the competencies of cybersecurity risk assessment. However, due to cyber security risk control specifically, many factors could be distinctive, such as specific technical skills required not only of IA but also the attention of the board/management that may set the tone from the top management level, provide support to cyber security risk assessment and completely cover and oversee its implementation (IIA, 2017b).

Internal Auditor's characterisations and competencies, in general, may be analysed from verities of perspectives, each of which may have its merit and demerit accordingly. Slapničar et al., (2022); and Vuko et al., (2021), group these perspectives into the process, output, and outcomes measures of the IAs attributes and competencies; process measures as based on the ground that IA is competence and adds values to the business if it complied with the ethics, values, standard in planning, performing engagements, and communicating audit findings (Islam et al., 2018b; Slapničar et al., 2022; Vuko et al., 2021). Nevertheless, this is the view

that IA competence is risk-based rather than control-based (Vuko & Slapnicar, 2021). Output measures of IA competencies relate to the capacity and ability of the IA to respond to auditee needs, mostly operationalized by the auditee's satisfaction and the percentage of recommendations enforced or implemented. Outcome on the other hand is based on the IAs' contributions to organizational task performance that may be inherently difficult to measure (Slapničar et al., 2022; Vuko & Slapnicar, 2021).

Studies by Vuko & Slapnicar, (2021) report that the output measure may be on the demand side or the user's perspective. They assumed that the IA is competent if it is consistence with the objectives, and the function is determined by the executive managers and the Board respectively (Islam et al., 2018a; Vuko et al., 2021).

Concerning the measurement of the cybersecurity risk assessment competencies and how effective IA meets the expectation of the Board and Management, the issue is that the board expectation may be vaguely defined or missing (IIA 2020). In a study of more than 1,100 Board members, only 9% of respondents said that their board have a very good understanding of cyber risk potential for impacting business operations (Slapničar et al., 2022; Vuko & Slapnicar, 2021). However, in most business organisations, issues of cyber security risk management and assurance end up being bottom-up driven (Slapničar et al., 2022; Vuko et al., 2022). Consequent to the outcome measurement model, that is, with some objective measures about success in mitigating cybersecurity risk and attacks, the issues may be twofold: the IA is not the only line of dedefenceand it contributes to better cybersecurity management only if its recommendations of findings are incorporated in the cybersecurity risk management model, and the second, the organization that may be exposed of the attractiveness of their digital assets might invest more in cybersecurity risk control but may surfer increase cyber-attacks (Slapnicer et al 2021).

Therefore, the process, output, and outcome approaches are in fact, not in conflict with one another as compliance with the standards required risk-based approaches and the integration of an organization's goals and board's expectations into the objectives of the IA. Consequent to the above, therefore, this study shall adopt the process approach which takes into account that in a rapidly evolving threats environment, competence cybersecurity assessment embraces best practices and state-of-the-art methods, that are risk-based, forward-looking, and proactive measures (Kahyaoglu, 2018; Slapničar et al., 2022; Vuko et al., 2022), which takes into account that in a rapidly evolving threats environment, an efficient cyber security risk assessment embraces and state-of-the-art methods (Islam et al., 2018a; Vuko et al., 2022).

2.8 CYBER SECURITY AND INFORMATION SHARING IN FINANCIAL BUSINESS ORGANIZATIONS

The first line of inquiry in cybersecurity looks at information exchange and its function in cyber-security which has reportedly grown crucial for accounting and public policy, according to earlier research. Information exchange and computer system security were compared in business organizations globally (Hausken,2017; Gordonetl.,2015). Their conclusions indicate that disclosing threats to and violations of computer security reduces the overall costs of reaching any specific degree of cybersecurity in the business entity. They, therefore, re-asserted that information exchange has been advocated as a key tool in promoting social well-being. Although their analysis indicated that information sharing may potentially lower overall security costs and increase societal welfare, there are some risks and full potential benefits from being realized.

These difficulties relate to the requirement for financial inducements to promote efficient cybersecurity-related information sharing. In other words, Gordon et a,l. (2003), proposes that business organization and society could gain from exchanging knowledge about cyber security breaches. Without the right financial incentives, companies can try to take advantage of others' security expenditures. In a similar vein, Gordon et al. (2003) hypothesized that a range of insider criminals, terrorists, or maybe a mix of them, frequently take advantage of the vulnerabilities to establish cyber-attacks. According to the authors, every business company should create a cyber-security program to prevent cyber-attacks. Although, this frequently has sporadic success due to difficult risk estimation and dynamic security environment. However, business organizations and other companies are not frequently proactive enough (Gordon et al., 2003, 2015). The current cyber-attacks on critical infrastructures are pretty well known. The USA (United States of America) they added, is already the country most dependent on information security systems. Thus, it is important to carefully analyze the effects of cybersecurity risks and information system vulnerability (Gordon et al., 2003).

Hausken, (2017), on the other hand, made the argument that weighing the merits and demerits of investing in cybersecurity and information sharing about other competitive advantage tactics. They stated that the strategies for information sharing and cyber security investment that are chosen by all actors including those who are players in the system, those who try to regulate and reshape it, and those who try to shut it down, determine how secure and

interconnected information system will be. This creates a role for public policy. They therefore, concluded that financial management systems in business organizations should be recognized as being important in the cyber security process.

Hausken (2007), however, argued that alternative tactics for gaining a competitive edge are interconnected with weighing the costs and advantages of information sharing and security investments. Hausken (2007) made the following claim: "The security of an interconnected information system depends on the strategies about information sharing and security investment chosen by all actors, including those who are players in it, those who attempt to regulate and reshape it-, and those who used it. Hausken (2017) stated information sharing increases linearly as the independence between an organizations is zero with negative or no independence. The independence between organizations that are not competitive is a fundamental determinant of info -formation sharing. Similarly, Gordon et al. (2015) noted that academics, government officials, and organisation leaders have encouraged the information exchange link to cybersecurity. The study further states that: the justification for information sharing is based on the idea that business may decrease their cybersecurity threat, vulnerabilities, and ultimately cyber incidences based on the experience of others in business organisations. They opined that from real options and standpoints information sharing with its ability to mitigate the risks associated with cybersecurity investment may well contribute to reducing the threats to private sector organizations' investment in cybersecurity management (Gordon et al., 2015). The study also made the case that the advantages of information sharing can operate as a critical motivator to get businesses to actively disclose their confidential data.

2.9 CYBERSECURITY INVESTMENT

The second research area focuses on cybersecurity investment. Given the importance of cybersecurity and ICT to ororganizations'erformance, the issue of how much money should be injected into cybersecurity-related activities has been raised frequently in extant studies (Ayoib & Salau 2022). Studies such as (Gordon et al., 2003V) initiated a model known as Gordon Leo Model which has gained much interest and publicity. The author asserted that cybersecurity is becoming a higher priority for most business organizations globally due to the nature of modern economies that are information incentives (Internet and World Wide Web) which has led them to develop an economic model that determines the real amount of investment in cybersecurity. They clarified that, under their paradigm, the words "cybersecurity and information security"

might be interpreted widely. In addition, Gordon et al. (2015) expand the Gordon Loeb Model to determine the ideal degree of investment in cybersecurity efforts, they look at how the presence of known externalities changes the maximum amount that a company should invest socially and optimally.

The findings indicate significant implications for practices because they show that underinvestment in cybersecurity activities by owners of an organization is practically inevitable unless they take into account the cost of breaches associated with externalities in addition to the cost brought on by breaches. Consequently, the authors concluded that inadequate investment in cybersecurity might seriously jeopardize both a countries and an organization's security and its ability to grow economically. Therefore, business organizations and countries across the globe are required to invest heavily to safeguard the security of information for economic prosperities (Gordon et al., 2015; Haapamäki & Sihvonen, 2019a; Steinbart &Raschke, 2018; Vuko et al., 2022). Similarly, extant studies in the areas of cybersecurity investment suggested the same highlights various findings. Hausken(2017) suggested that businesses are increasingly investing in security technologies due to the possibility of cyber-attacks. The magnitude of the investment is determined using principles. Laws, however, also have an impact on the incentives for businesses to invest in security systems. The SOX established stringent restrictions, as was already mentioned When the average attack level is 25% of the firm's needed rate of return (Hausken,2017), busi-nesses invest in notion security. They underlined that "any firm invests in security technology when the needed rate of return from security investment exceeds the average attack level, or when the formal control requirements compel investment."

2.10 INTERNAL AUDITING, CONTROLS AND CYBERSECURITY

Under this stream of the study, Pathak (2005) illustrates how technology convergence affects a company's internal control mechanism and stated that an auditor must be aware of security risks that the financial information system or possibly, the entire organizational information system faces. To contextualize the security system design and organizational vulnerabilities in the context of integration of complex IT into business processes, Pathak (2005) tried to do so. The study emphasized the need for auditors to be aware of technology risk management with basic characteristics, and its effects on organizational vulnerabilities and internal controls. However, a study (Hausken, 2017), reports that management of applicable

and acceptable IT governance and control practices is required with basic attributes to enhance the previous and budgeted IT environment.

2.11 CYBERSECURITY ACTIVITIES AND DISCLOSURE

This is another stream of security literature which contained articles investigating the disclosure of cybersecurity activities. Gordon et al (2006) examine the effect of the SOX (2002) on voluntary disclosure of IT security activities by organizations. The study vividly stated that SOX had a positive effect on the disclosures. Comprehensively, their results iicates the countary disclosure of information security activities had improved by over 100 % the era of SOX when compared with the previous two years before the era of the SOX law implementation. This was favourable dings as SOX failed to completely solve the problem of information security. On the other hand, Gordon et al.,(2003, 2015) investigates the voluntary disclosure of cybersecurity and affirmed that voluntary disclosure of cybersecurity in yearly reports enable the business organization to provide signs to the markets in which the company is truly involved in ascertaining, preventing and mitigating cybersecurity breaches. Consequently, the study suggests that it is a means taken whether or not a company or organization voluntarily decides to disclose issues pertaining to information security that are related cybersecurity. In addition, the study proved empirical evidence for the debated that voluntary disclosures relating to cybersecurity positively and significantly associated to mthe arket price of stocks. The study outcome reveals generic support for the signalling argument that indicates that the manager who discloses information security voluntarily are in turn enhancing organization values. More importantly, the study indicates that voluntary disclosures associated with proactive cybersecurity strategies by organizations have more effects on the organization's stock market (Gordon et al., 2003, 2015).

Lan et al. (2013) investigate the relationship between the disclosures and the actualization of cybersecurity risk and reports that organization always disclose cybersecurity risk factors in public documents. The study argued that the internal cybersecurity information related to disclosure can be positive or negative (Lan et al., 2013). They also examine the nature of disclosed cybersecurity risk elements, taken to represent the organization report concerning information security.

On the other hand, Li & Liu. (2021) examine if ccybersecurity disclosures are reports for further cybersecurity attacks. They concentrate on two main strategies: the presence of

cybersecurity risks disclosure and the time of cybersecurity risk disclosure. The study indicates that the presence of the risk elements in the earlier stage and the length of these risk disclosure element are associated with future information about cybersecurity. The results also reveal that the relationship between the available cybersecurity risk become minimal after the time of the USA Security and Exchange Commission's (SEC) cybersecurity disclosure rules and regulations comes into effect. This informed why Li & Liu. (2021) work agrees with SEC's position on underlying cybersecurity risk assessment. Although, the study reveals that the SEC's disclosure strategies may unintentionally motivate organisations to assess cybersecurity risks despite the rate and level of risks.

Studies such as Bade & Mohammed (2019), investigated trade confidential and cybersecurity attacks and the relationship between organization disclosure in form 10-k among existing trade confidentialities and cybersecurity attacks otherwise referred to as breaches. The study added to the empirical study by targeting mainly breaches or attacks which focus on trade confidentialities, the results indicates that organization which mention the existence of trade confidentiality positively and significantly enhance the probability of being attacks than other organization with less or no such attention. The outcome of the study was however strong among infant companies, companies with fewer employees and companies operating in industries with little concentrations.

2.12 CYBERSECURITY THREATS AND BREACHES

Extant studies on cybersecurity threats and breaches examine information movement among internet organizations. The concepts of internet organization sees it as all organizations which operate in different types of companies, but are the same in their total dependence on information technology when carrying out critical fundamental assignments or operations and commerce (Brogi et al., 2018). The study investigates the stock markets about denial service on certain internet organization and attacks. The study indicates that negative means and abnormal gains occurred among internet organizations which were not attacked. Of greater interest, the attacks happened both in internet organization such some companies were attacked and in the internet organization where no companies were attacked. Consequently, they opined that internet companies were the same in size to those which were more probably to be affected in the future. In the same vein, Boritz and No (2005) examine scybersecurity threats as well as the limitations of security technology.

Additionally, to ensured reliability, the studied security requirements, trustworthy financial-based organizations disclosure services. In conclusions, their studies reveals that several proposed security standards and opinions indicates that Web Security Architecture as a reliable strategies for financial- based reporting services. On the other hand, Abu-Musa (2006)) examine the perceived security threats to defined accounting information system (MIS) in Egyptian banking organizations and stated that ‘’ advance technology has created positive significant risk associated to devised a mean for the augured of the integrity, confidentiality and availabilities of IT system”. Although, the result indicates that the wrong entry of data by employees, with the accidental destruction of the data by employees couple with the initiation and addition of computer viruses to the information system and natural human –made attacks, with wrong passwords sharing and wrong printing and sharing of information of malicious insiders are said to have the most significant cybersecuirty risks. Unfortunately, the outcome discloses that the higher security concerns are said to have emanated from within other than outside the financial–based organizations.

Furthermore, scholars have examine cybersecuity risk , breaches and attacks on stock market gains of organizations (Islam et al., 2018; Khando et al., 2021; Kure & Islam, 2019; Shankaraiah, K. & Amiri, 2017). They held that cybersecurity attacks are related to the decline of almost 3.6 per cent stock value in the month as the attacks are disclosed. Therefore, financial-based organizations have the responsibility of mitigating the incidence of cybersecurity risk and attacks (Abu-Musa, 2006).

3 METHODOLOGY OF THE STUDY

The literature review method of extant studies relating to internal auditors’ characterization and cybersecurity risk assessment with the intervening role of cybersecurity threats awareness was adopted. Therefore, through this method, the study got an insight into the level of studies relating to internal auditors’ attributes and how it influences the cybersecurity risk assessment in the financial-based business organization.

4 CONCLUSIONS AND RECOMMENDATIONS

The significance of cybersecurity management to financial organizations’ critical infrastructures such as banking institution and their customers for the protection of the integrity,

confidentiality, and availability of information technology informed the need for the conceptualization of the subject matter to be studied. Consequently, upon the advancement of information communication technology with numerous opportunities for the ease of business and a shift from analogue to digital modes of business transaction and public service delivery, companies are changing their mode of service delivery and customers call for the protection of their classified information from the attack of cybercriminals and malicious insiders with a relationship with customers information make it a necessity for more attentions of the board over their primary assignment (financial auditing and investigation) to the proactive role of cybersecurity risk management. That is the function of the internal auditors in an organization that has moved from traditional financial reporting to the security of classified and critical infrastructure of the organization through cybersecurity risk assessment for board strategic planning and budgeting. This is however, highlighted to have constituted major challenges to professionals accountant as studies have reported that most employees such as the internal auditors' lack the required competencies to embark on task performance as cybersecurity risk assessment (Dellai, 2015; Haapamäki & Sihvonen, 2019a, 2019b; Ismail, 2021; Kure & Islam, 2019; Zwilling, 2022), hence, the rise in the incidence of cybersecurity attacks in public and private companies in a developed and underdeveloped economy.

Within the ambit of such views, internal auditors' characterization appears to be a significant determinant of both cybersecurity risk assessment and cybersecurity threats awareness (Betti & Sarens, 2020a; Mahoney et al., 2013; Steinbart & Raschke, 2018; Zwilling, 2022). Consequently, this paper aims to conceptually examine cybersecurity risk assessment putting into consideration the influence of the internal auditor's characterization such as the professional ethics of integrity and objectivity, personality traits, professional skills and knowledge competencies, deterrence and rewards with the mediating role of the cybersecurity threats awareness in the public listed banking companies in Nigeria. To this end, based on the extant studies' outcome which was mostly in a developed economy, internal auditors' characterization has influenced task performance cybersecurity risk management through mixed findings. As an addendum to the body of knowledge and literary studies on empirical evidence regarding the relationship between internal auditors and cybersecurity risk assessment, this study dwelled on the relationship between internal auditors' characterization and cybersecurity risk assessment with mediating role of cybersecurity threats awareness and conceptually concludes as follows:

(1) Research on internal auditors' characterization and cybersecurity risk assessment is still scanty in most developing economies the academic industry (2) Proposes a positive association between the reviewed internal auditors' characterizations (such as the professional ethics of integrity and objectivity, personality traits, professional competencies of skills and knowledge, deterrence and rewards and cybersecurity risk assessment), (3) That cybersecurity threats awareness mediate the relationship between the internal auditor's characterization and cybersecurity risk assessment (Betti & Sarens, 2020b; Haapamäki & Sihvonen, 2019b; Islam, 2019; Mahoney et al., 2013; Salleh & Aziz, 2014; Steinbart et al., 2015; Steinbart & Raschke, 2018; Vuko & Slapnicar, 2021). Therefore, this paper adds to the body of knowledge and literary study that have need documented to be scanty in the academic industry through the examination of the internal auditor's characterization in terms of cybersecurity risk assessment in the context of this study. Hence, extant studies mostly dwelled on the internal audit function and firm performance, earnings management financial reporting firm values and others. Theoretically, the study equally contributes to knowledge and literary studies through the examination of competency and reasoned action theories as a determinant of internal auditors' characterization in task performance cybersecurity risk assessment (Özçelik & Ferman, 2006; McClelland, 1973; Sunyoto, 2020; Ajzen, 1991). Not that all, the study also has a practical significance and implication for the government banking institution board, cybersecurity and information management officers, chief audit executives, regulators, bank customers and other stakeholders, financial analysts and the academia in terms of policy formulation and further research in the areas of cybersecurity risk management. Such could enhance the mitigation and monitoring of cybersecurity attack incidence in Nigeria specifically and the global economy in general.

The study, however, suffers some limitations. The internal auditor's characterization examined and reviewed are just a few of the others that could be examined in terms of cybersecurity risk assessment. Nevertheless, this study is a conceptual work, therefore, an empirical examination is very significant and required to advance the causal effect between internal auditors' characterization and cybersecurity risk assessment. Consequently, the study recommends that future examinations be empirical and should add other internal auditor characterization such as education, experience, cybersecurity policy and external auditors' contribution and information communication standards with another construct in examining cybersecurity risk assessment and internal auditors characterization. Other economic

environments can also be of importance from a comparative perspective, particularly an emerging economy.

REFERENCES

Abu-Musa, A. A. (2006). Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations. *Journal of King Saud University - Computer and Information Sciences*, *18*, 1–30. https://doi.org/10.1016/s1319-1578(06)80001-7

Ajiji, Y. M. (2019). Cybersecurity Issued in Nigeria and Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available*, *7*(April 2017). https://doi.org/10.23956/ijarcsse/V6I12/01204

Ajzen, I. (1991). The theory of planned behabehaviour*urnal of Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Albawwat, I.E., Al-Hajaia. M.E.,& Al Frijat, Y. . (2021). The Relationship Between Internal Auditors' Personality Traits, Internal Audit Effectiveness, and Financial Reporting Quality: Empirical Evidence from Jordan. *Journal of Asian Finance, Economics and Business*, *8*(4), 797–808. https://doi.org/10.13106/jafeb.2021.vol8.no4.0797

Aldasoro, I., Gambacorta, L., & Giudici, P. (2020). Operational and cyber risks in the financial sector. *Journal of Accounting and Economics*, *8*.

Alhazmi, A. K. (2015). Conceptual Model for the Academic Use of Social Networking Sites from Student Engagement Perspective. *Conference on E-Learning, e-Management and e-Services (Pp. 1–6). Institute of Electrical and Electronics Engineers Inc. Https://Doi.Org/10.1109/IC3e.2014.7081232*, *April*. https://doi.org/10.1109/IC3e.2014.7081232

Alih Usman, Samuel, P. & Sadiq, H. (2019). Job Satisfaction and Workers Performance in Kogi State Public Sector.Journal of Leadership Accounting Development and Investigation Research (JLADIR).Vol.1 July 2019.

Ayoib Che-Ahmad & Salau Olarinoye Abdulmalik (2022). IT investment and corporate performance: Evidence from Malaysia, Cogent Business & Management, 9:1, 2055906, DOI: 10.1080/23311975.2022.2055906

Babo,S.Alon,I.& Paltrinieri, A (2020). Corruption in international business: A review and research agenda.International Business Revie 29/4

Bade, A. M., & Mohammed, I. (2019). Cybersecurity Capability Maturity Model for Critical Information Technology Infrastructure Among Nigeria Financial Organisation. *International Journal of Current Research*, *11*(06), 06. https://doi.org/https://doi.org/10.24941/ijcr.35585.06.2019

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social

psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

Betti, N., & Sarens, G. (2020a). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change © EmeraldPublishingLimited 1832-5912 DOI 10.1108/JAOC-11-2019-0*. https://doi.org/10.1108/JAOC-11-2019-0114

Betti, N., & Sarens, G. (2020b). *Understanding the internal audit function in a digitalised business environment*. https://doi.org/10.1108/JAOC-11-2019-0114

Bidabad, B., & Sherafati, M. (2016). Operational ethical banking in Rastin Banking: (Professional ethics, auditing, inspection, control, monitoring and preservation). *International Journal of Law and Management*, *58*(4), 416–443. https://doi.org/10.1108/IJLMA-07-2015-0037

Bondarenko, N., & Kryzhanovska, O. (2020). Professional Values and Ethics as a Factor of Increasing Trust in the Profession of the Accountant. *Accounting and Finance*, *4*(4(90)), 10–16. https://doi.org/10.33146/2307-9878-2020-4(90)-10-16

Brogi, M., Arcuri, M. C., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership and Control*, *15*(2), 70–83. https://doi.org/10.22495/cocv15i2art6

Carlton, M., & Levy, Y. (2017). *Cybersecurity skills : Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation*. *5*(2), 16–28.

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. *Journal of Information and Computer Security*, *27*(1), 101–121. https://doi.org/10.1108/ICS-11-2016-0088

Clarkson, P. M., Li, Y., Richardson, G. D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis. *Accounting, Organizations and Society*, *33*(4–5), 303–327. https://doi.org/10.1016/j.aos.2007.05.003

Czerniawska, M., & Szydło, J. (2021). Do values relate to personality traits and if so, in what way? – analysis of relationships. *Psychology Research and Behavior Management*, *14*, 511–527. https://doi.org/10.2147/PRBM.S299720

Dellai, H. (2015). Factors Affecting the Internal Audit Effectiveness. *Factors Affecting the Internal Audit Effectiveness*, *12*(2), 89–109. https://doi.org/10.14710/jaa.v12i2.13860

Dzikrullah, A. D., Harymawan, I., & Ratri, M. C. (2020). Internal audit functions and audit outcomes: Evidence from Indonesia. *Cogent Business and Management*, *7*(1). https://doi.org/10.1080/23311975.2020.1750331

Elaigwu Moses, Ayoib Che-Ahmad & Salau Olarinoye Abdulmalik | (2020) Board governance mechanisms and sustainability reporting quality: A theoretical framework, Cogent Business & Management, 7:1, 1771075

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6), 461–485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, *06*(01), 24–30. https://doi.org/10.4236/jis.2015.61003

Haapamäki, E., & Sihvonen, J. (2019a). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Haapamäki, E., & Sihvonen, J. (2019b). Research on International Standards on Auditing: Literature synthesis and opportunities for future research. *Journal of International Accounting, Auditing and Taxation*, *35*, 37–56. https://doi.org/10.1016/j.intaccaudtax.2019.05.007

Hamshari, Y. M. (2021). The Relationship of Professional Skepticism to the Risks of Auditing and Internal Control and the Discovery of Fraud and Core Errors in the Financial Statements in Jordan. *Academic Journal of Interdisciplinary Studies Www.Richtmann.Org Vol 10 No 2 March 2021 Research*, *2*(2281–3993), 105–117.

Hausken, K. (2017). Information Sharing Among Cyber Hackers in Successive Attacks. *International Game Theory Review*, *May*. https://doi.org/10.1142/S0219198917500104

IFAC. (2011). IFAC Sustainability Framework 2.2.0 Noitle. In *PAIB Committee*.

IFAC. (2015). *IES 3 - Professional Skills and General Education*. 58–64. https://www.ifac.org/system/files/publications/files/ies-3-professional-skills-1.pdf

IIA. (2017a). *Measuring Internal Audit Effectiveness and Efficiency*.

IIA. (2017b). Measuring Internal Audit Effectiveness and Efficiency. In *International Professional Practices Framework, The Institute of Internal Auditors* (Issue December).

Islam, S. (2019). *Md. Shariful Islam, DBA, CPA, CMA*. 1–4.

Islam, S., Farah, N., & Stafford, T. F. (2018). Factors associated with ssecurity/cybersecurityaudit by internal audit function An international study. *Managerial Auditing Journal*, *33*(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595

Ismail, I. A. (2021). *Understanding quantitative and qualitative research methods : A theoretical perspective for young researchers Understanding QuaQuantitative andalitative ResearchMethods : A TheoreticalPerspective for Young Researchers*. *February*, 70–87. https://doi.org/10.2501/ijmr-201-5-070

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kuijck, B. Van, & Paresi, V. (2020). Personality of internal auditors ; an exploratory study in

The Netherlands Relevance to practice Keywords. *Aandblad Voor Accountancy En Bedrijfseconomie 94(3/4) (2020): 113–125 DOI 10.5117/Mab.94.47818 Research Article Personality*, *94*, 113–125. https://doi.org/10.5117/mab.94.47818

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications*, *4*, 332–340. https://doi.org/10.1049/iet-cps.2018.5079

Lan, Y., Wang, L., & Zhang, X. (2013). Determinants and features of voluntary disclosure in the Chinese stock market. *China Journal of Accounting Research*, *6*(4), 265–285. https://doi.org/10.1016/j.cjar.2013.04.001

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security ; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, *13*(1), 25. https://doi.org/10.1504/IJMFA.2021.116207

Luthan, E., Ali, S., & Hairaty, E. (2019). the Professionalism, Competence, Organizational Commitment & Job Satisfaction on the Performance of Auditor. *The International Journal of Business Review (The Jobs Review)*, *2*(2), 87–104. https://doi.org/10.17509/tjr.v2i2.21345

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, *63*(December 2019), 101382. https://doi.org/10.1016/j.techsoc.2020.101382

Mahoney, L. S., Thorne, L., Cecil, L., & LaGore, W. (2013). A research note on standalone corporate social responsibility reports: Signaling or greenwashing? *Critical Perspectives on Accounting*, *24*(4–5), 350–359. https://doi.org/10.1016/j.cpa.2012.09.008

Marei, A., Mustafa, J. A., Othman, M. D., Daoud, L., Lutfi, A., Al-Amarneh, A. (2023) The Moderation of Organizational Readiness on the Relationship Between Toe Factors and Fintech Adoption and Financial Performance. Doi: https://doi.org/10.26668/businessreview/2023.v8i7.2800

McClelland, D. C. (1973). Testing for competence rather than for "intelligence". *Journal of American Psychologist*, *28*(1), 1–14. https://doi.org/10.1037/h0034092

Mooradian, T., Renzl, B., & Matzler, K. (2006). Who trusts? Personality, trust and knowledge sharing. *Management Learning*, *37*(4), 523–540. https://doi.org/10.1177/1350507606073424

NIST. (2018). NIST Cybersecurity Framework Assessment for [Name of company]. *NIST*, *1105*.

Özçelik, G., & Ferman, M. (2006). Competency Approach to Human Resources Management: Outcomes and Contributions in a Turkish Cultural Context. *Human Resource Development*

Review, *5*(1), 72–91. https://doi.org/10.1177/1534484305284602

Pasculli, L. (2020). *The Global Causes of Cybercrime and State Responsibilities . Towards an Integrated Interdisciplinary Theory*. *2*(April).

Pérez-sánchez, B., González, M., & Perea, C. (2021). *A New Computational Method for Estimating Simultaneous Equations Models Using Entropy as a Parameter Criteria*. 1–9.

Poorchangizi, B., Borhani, F., Abbaszadeh, A., Mirzaee, M., & Farokhzadian, J. (2019). The importance of professional values from nursing students' perspective. *BMC Nursing*, *18*(1), 1–7. https://doi.org/10.1186/s12912-019-0351-1

Pricewaterhouse Coopers, P. (2017). *COSO Internal Control Framework.*

Products, G., Bochkovskyi, A., & Sapozhnikova, N. Y. (2018). *THE THEORY AND PRACTICE OF RISK ASSESSMENT OF PROFESSIONAL THE THEORY AND PRACTICE OF RISK ASSESSMENT*. *July*. https://doi.org/10.15673/gpmf.v18i2.948

Radoilska, L., & Ceva, E. (2021). *Ethical Theory and Moral Practice at 24 Content courtesy of Springer Nature , terms of use apply . Rights reserved . Content courtesy of Springer Nature , terms of use apply . Rights reserved* . 1–3.

Şahin, R., Öztürk, Ş., & Ünalmiş, M. (2009). Professional ethics and moral values in Akhi institution. *Procedia - Social and Behavioral Sciences*, *1*(1), 800–804. https://doi.org/10.1016/j.sbspro.2009.01.143

Salleh, K., & Aziz, R. A. (2014). Traits , skills and ethical values of public sector forensic accountants : an empirical investigation. *Procedia - Social and Behavioral Sciences*, *145*, 361–370. https://doi.org/10.1016/j.sbspro.2014.06.045

Shankaraiah, K. & Amiri, S. M. S. (2017). Audit committee quality and financial reporting quality: a study of selected Indian companies. *Journal of Accounting and Business Dynamics*, *4*(1), 1–18.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*(June 2020), 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Soto, C. J., & Jackson, J. J. (2013). Five-Factor Model of Personality. *Psychology*, *January 2020*. https://doi.org/10.1093/obo/9780199828340-0120

Soto, C. J., & John, O. P. (2009). Ten facet scales for the Big Five Inventory: Convergence with NEO PI-R facets, self-peer agreement, and discriminant validity. *Journal of Research in Personality*, *43*(1), 84–90. https://doi.org/10.1016/j.jrp.2008.10.002

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2015). The Influence of Internal Audit on Information System Effectiveness: Perceptions of Internal Auditors. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2685943

Steinbart, P. J., & Raschke, R. L. (2018). The Relationship between Internal Audit and Information Security : An Exploratory Investigation The Relationship between Internal

Audit and Information Security : An Exploratory Investigation. *Journal of Accounting and Economics (2017) 5(May) 200Accounting, Organizations and Society*, *1685*(515).

Sunyoto, Y. (2020). Auditor's experience, professional commitment, and knowledge on financial audit performance in indonesia. *International Journal of Economics and Business Administration*, *8*(2), 191–199. https://doi.org/10.35808/ijeba/451

Suzuki, M., Ando, N., & Nishikawa, H. (2022). Discontinuity of required oral and literacy skills across job roles in achieving high work performance: An fsQCA approach. *International Business Review*. https://doi.org/10.1016/j.ibusrev.2022.102072

Tedeholm, P. G., Sjöberg, A., & Larsson, A. C. (2021). Personality traits among Swedish counterterrorism intervention unit police officers: A comparison with the general population. *Personality and Individual Differences*, *168*(September 2020), 110411. https://doi.org/10.1016/j.paid.2020.110411

Tehranineshat, B., Torabizadeh, C., & Bijani, M. (2020). A study of the relationship between professional values and ethical climate and nurses' professional quality of life in Iran. *International Journal of Nursing Sciences*, *7*(3), 313–319. https://doi.org/10.1016/j.ijnss.2020.06.001

Thompson, E. C. (2018). Cybersecurity Incident Response, How to Contain, Eradicate, and Recover from Incidents. In *Apress*.

Usman Alih, Elaigwu M. &Salau R.K. (2021).Cybersecurity Risk Assessment and The Role of Internal Audit Function Among The Listed Financial Companies in Nigeria: A Global Empirical Perspective.Creative Journal of Business Research. Vol.1.No.1 2021

Vuko, T., Cular, M., & Dra, M. (2022). *International Journal of Accounting Effectiveness of cybersecurity audit*. *44*(January 2021). https://doi.org/10.1016/j.accinf.2021.100548

Vuko, T., & Slapnicar, S. (2021). *Key Drivers of Cybersecurity Audit Effectiveness : a neo-institutional Key Drivers of Cybersecurity Audit Effectiveness : a neo-institutional perspective*. *October*.

Yanita., Yusniar., Iis, E. Y., Abubakar, R., Maimunah, S. (2023) The Effect of Information Technology Utilization and Employee Competence on Employee Performance with Job Satisfaction as the Intervening Variable in the Aceh Irrigation Service,International Professional Business Review Journal:Doi: https://doi.org/10.26668/businessreview/2023.v8i7.2564

Yunus, M. R. B. M., Wahab, N. B. A., Ismail, M. S., & Othman, M. S. (2018). The Importance Role of Personality Trait. *International Journal of Academic Research in Business and Social Sciences*, *8*(7), 1028–1036. https://doi.org/10.6007/ijarbss/v8-i7/4530

Zweighaft, D. (2017). Business email compromise and executive impersonation : are financial institutions exposed ? *Journal of Investment Compliance*, *18*(1), 1–7. https://doi.org/10.1108/JOIC-02-2017-0001

Zwilling, M. (2022). Trends and Challenges Regarding Cyber Risk Mitigation by CISOs — A Systematic Literature and Experts ' Opinion Review Based on Text Analytics. *Journal*

Accounting and Electronic Risk Management.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness , Knowledge and Behavior : A Comparative Study Cyber Security Awareness , Knowledge and Behavior : A Comparative Study Moti Zwilling , Galit Klien , Dušan Lesjak , Łukasz Wiechetek , Fatih Cetin &. *Journal of Computer Information Systems*, *00*(00), 1–16. https://doi.org/10.1080/08874417.2020.1712269