Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE IMPACT OF GENDER MODERATION ON AUDITORS' INTENTION TO ADOPT CYBERSECURITY: A TAM AND PMT FRAMEWORKS APPROACH

BAGAS INDRA PRANATA[1], FIDELA ANDINA[2], IGNATIUS EDWARD RIANTONO[3]

[1]Accounting Department, School of Accounting, Bina Nusantara University, Jakarta, Indonesia, 11480

[2]Accounting Department, School of Accounting, Bina Nusantara University, Jakarta, Indonesia, 11480

[3]Accounting Department, School of Accounting, Bina Nusantara University, Jakarta, Indonesia, 11480

E-mail: [1]bagas.pranata@binus.ac.id, [2]fidela.andina@binus.ac.id, [3]iriantono@binus.edu

ABSTRACT

The growing complexity of cyber threats in the auditing environment has intensified the need to understand the factors that drive auditors to adopt cybersecurity technologies. This study explores the impact of gender moderation on auditors' intention to adopt cybersecurity technologies by utilizing the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT). A quantitative approach was employed, with data collected from 429 auditors working in public accounting firms across Indonesia through structured questionnaires. After excluding 16 outliers with highly fluctuating responses, the final sample consisted of 413 respondents. Structural Equation Modeling-Partial Least Squares method (PLS-SEM) was employed using SmartPLS to analyze the data. The findings indicate that Perceived Usefulness, Perceived Severity, Perceived Vulnerability, Perceived Response Efficacy, and Perceived Self-Efficacy significantly influence auditors' intention to adopt cybersecurity technologies. However, Perceived Ease of Use does not have a significant impact. Additionally, gender did not moderate the relationship between these factors and auditors' adoption intention. These results suggest that although perceptual differences between male and female auditors exist, they are not substantial enough to warrant gender-specific cybersecurity adoption strategies. Therefore, cybersecurity implementation policies can be applied universally across auditors irrespective of gender.

Keywords: *Cybersecurity, Audit Technology, Data Security, Technology Acceptance Model, Protection Motivation Theory*

1. INTRODUCTION

In the era of digital transformation, it is crucial for organizations to prioritize cybersecurity measures and ensure that their systems are protected from potential threats. Cybersecurity has evolved into a significant challenge for companies, and maintaining organizational continuity, including for those in the audit profession [1]. According to [2], developments in the industrial revolution 4.0 era have encouraged one of the four largest public accounting firms to invest in the implementation of technology that is expected to advance global productivity in the business world by 2030 to $ 6.6 trillion. PwC's "2024 Global Digital Trust Insights" report, which surveyed over 3,876 business and technology executives from leading global companies, highlights that cybersecurity is now a top priority, with increased budget allocations for information technology (IT), operational technology (OT), and automation, and reveals an average data breach cost of approximately IDR 15 billion [3]. Data shows that 35% of organizations in the Asia-Pacific region have experienced data breaches resulting in losses between USD 1 million and USD 20 million, and in response to the growing number of major breaches over the past three years, 84% of business and technology executives in Asia-Pacific have increased their cybersecurity budgets, with 54% of organizations prioritizing the protection of customer, employee, and transactional data as cybersecurity risks continue to rise [4]. Subianto, Head of Digital and Technology at PwC Indonesia, notes that regulators in Indonesia are increasingly addressing cybersecurity in response to rising threats [5]. For example, the Financial Services Authority (OJK) has tightened cybersecurity

regulations through Circular No. 29/2022 for commercial banks [6].

As the complexity of the business environment increases and the demand for greater data transparency grows, auditors are encouraged to adopt modern technologies, such as artificial intelligence and digital security systems, to improve audit efficiency and ensure long-term quality [7]. Previous research explains that collaboration between auditors and technology plays an important role in improving data accuracy and audit performance [8], [9]. Regulators can also support policies enhancing auditor performance, especially as cybersecurity becomes a critical focus of external audits due to rising cyber threats and regulatory pressures. External auditors now assess both financial health and cybersecurity risks, with cyber events influencing financial reporting, audit risk, fees, and workload [10]. Cybersecurity is defined as the harmonization of capabilities in people, processes, and technologies to secure and control both authorized and unauthorized access to electronic computing systems [11]. Moreover, the integration of cybersecurity measures into audit practices is not only a response to external pressures but also a proactive strategy to bolster the credibility of audit findings. The AICPA has introduced frameworks for voluntary cybersecurity revelations, which auditors can leverage to improve transparency and stakeholder trust [12]. This is particularly relevant in the context of SAP systems, where the complexity of data management necessitates stringent security protocols. Almufareh and Humayun argue that effective security practices must be embedded in the software development process to mitigate risks associated with SAP deployments [13]. The adoption of advanced audit technologies and techniques, such as continuous monitoring and data analytics, allows external auditors to conduct more thorough and efficient cybersecurity assessments [14]. These technologies enable auditors to identify anomalies and potential security breaches more effectively, thereby improving the overall quality of the audit [14]. This definition underscores the multidisciplinary nature of cybersecurity, to effectively address the challenges posed by cyber threats [15].

This study employs the technologies Acceptance Model (TAM) and Protection Motivation Theory (PMT) to analyse the determinants affecting auditors' intentions to utilise cybersecurity technologies [16]. The Technology adoption Model (TAM) was chosen because it is a well-recognized framework for analysing user adoption of technology. TAM, initially formulated by Davis in 1986, asserts that perceived usefulness and perceived ease of use substantially affect users' intentions to accept and employ technology [17], [18]. Simultaneously, the Protection Motivation Theory (PMT) functions as a crucial foundation for comprehending users' intents to use cybersecurity measures. Protection Motivation Theory includes two dimensions: threat assessment and coping assessment [19]. In simpler terms, individuals' protective motive behaviour in response to perceived threats is shaped by threat appraisal and coping appraisal. Threat appraisal encompasses perceived vulnerability and perceived severity. Coping appraisal is the amalgamation of response efficacy and self-efficacy in addressing the perceived threat [20]. Utilising these two models, researchers may examine the adoption of new technology (TAM) and the reaction to security threats (PMT) that affect auditors' judgements.

In addition, this study employs gender as a moderating variable to examine how differences in perceptions between men and women regarding technology and threats affect the relationship between TAM and PMT factors and the intention to use cybersecurity. Bem explains the gender schema theory posits that gender stereotypes emerge from the cognitive processing of information through schemas or associations pertaining to gender. This theory emphasizes the classification of the world into two gender categories, masculinity and femininity, based on cultural constructs, without scrutinizing the substance or particular meanings of these categories [21]. Hossain explains the term "gender" as a societal paradigm for interpreting men and women in relation to certain physical characteristics, including personal beliefs, roles, attitudes, and behaviors [22]. Research indicates that gender plays a critical role in shaping cybersecurity beliefs and behaviors. For instance, Anwar et al. found that gender significantly moderates the relationship between psychosocial factors and self-reported cybersecurity behaviors, suggesting that male and female employees may respond differently to cybersecurity initiatives and training programs [16]. This aligns with findings from Lee and Chua, who reported that female respondents exhibited lower levels of cybersecurity knowledge compared to their male counterparts, which could hinder their intentions to adopt cybersecurity technologies [23]. Furthermore, Addae et al. highlighted those men generally reported higher self-efficacy in cybersecurity behaviors than women, indicating a potential barrier

for female auditors in adopting new cybersecurity technologies [24].

Previous studies on the intention to adopt new technology within audit procedures have utilized the Technology Acceptance Model [25], [26], [27]. However, to the best of our knowledge, no comprehensive review has examined recent research addressing the intention to adopt cybersecurity through the dual dimensions of the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT). Consequently, our objective is to explore how the independent variables derived from TAM and PMT impact users' intentions to adopt cybersecurity practices in external audit processes, particularly focusing on client financial data security. In addition, we also analyzed the impact of gender differences on the relationship between factors from the TAM and PMT frameworks with auditors' intention to adopt cybersecurity. Through this integrated model, the study will examine both the perceived ease of use and usefulness of cybersecurity tools (TAM) alongside threat and coping appraisals (PMT). This research also seeks to provide deeper insights that can guide external auditors in developing more inclusive and relevant cybersecurity adoption strategies while offering organizations actionable strategies to implement cybersecurity technologies in future audit procedures.

2. LITERATURE REVIEW

2.1 Cybersecurity in Auditing

Cybersecurity enforces policies, procedures, and technical measures to safeguard, identify, rectify, and defend against the destruction, unauthorized access or alteration, or exploitation of information and communication systems and their contained information. Cybersecurity has become an essential component in modern auditing practices to ensure data confidentiality and prevent cyber threats [28]. The swift advancement of technology and innovation, along with the changing landscape of cyber threats, exacerbates the situation. In response to these extraordinary challenges, auditors will embrace cybersecurity tools to effectively manage risks and boost security [29]. In the realm of cybersecurity, particularly concerning client data security, organizations face a myriad of challenges that necessitate a comprehensive understanding of both the threats and the protective measures available. The increasing reliance on digital systems across various sectors has heightened the risk of cyberattacks targeting sensitive client information. This situation underscores the importance of implementing robust cybersecurity practices to mitigate potential damage from such attacks. Research indicates that cybersecurity awareness among employees plays a crucial role in reducing the impact of cyber threats. For instance, Alharbi et al. highlight that organizations with employees who possess adequate cybersecurity knowledge are more likely to report data breaches, thereby facilitating timely responses to potential threats [30].

2.2 Technology Acceptance Model

The rapid technological advancements of the 1970s, many companies faced difficulties in adapting to system failures [31]. In response to the rising incidence of system failures, many researchers commenced investigations into the field of system prediction [32]. The Technology Acceptance Model (TAM) was initially formulated by Davis, proposing a theoretical framework for comprehending human behavior in the acceptance and utilization of technology [33]. Davis posited that system usage is a behavior motivated by users and immediately affected by external stimuli, such as the system's components and efficiency [31]. The Technology Acceptance Model (TAM), as articulated by [34], posits that users will recognize the utility of technology based on its simplicity of use, which subsequently increases their willingness to adopt it. This aligns with findings from research [35], TAM explains that the perceived usefulness and ease of use of these technologies can influence an organization's willingness to adopt cybersecurity. Employees are more likely to adopt and utilize new technology when they recognize that it will enhance their productivity and simplify their tasks [36]. This has resulted in considerable theoretical and empirical support, establishing it as the most robust paradigm for elucidating the adoption behaviours of information technology [18].

The perceived ease of use (PEOU) is a critical factor influencing individuals' intention to use technology. Davis emphasized that when a user perceives a system as simple and straightforward, their intention to use it increases significantly [33]. Venkatesh and Bala's research emphasizes that perceived ease of use is a determinant of technology acceptance, suggesting that users are more likely to engage with technology that they perceive as user-friendly [37].

Perceived Usefulness refers to an individual's belief that using a specific technology will enhance their job performance. Davis also emphasized that users are more likely to adopt technologies they perceive as beneficial for achieving their tasks efficiently [33]. Venkatesh and Davis also noted that while perceived ease of use has shown variable effects on intention, perceived usefulness remains a more consistently significant predictor of technology acceptance [18].

The intention to use technology refers to the probability that an individual will employ a given technology, leading to the behaviour of utilising that technology [38].

2.3 Protection Motivation Theory

The PMT model, originally formulated by Ronald Rogers in 1975, sought to elucidate the mechanisms by which individuals are driven to safeguard themselves against various perceived health dangers [20] as cited in [39]. Protection Motivation Theory (PMT) is one of the most widely used theories in explaining users' technology acceptance behavior. Initially, this model includes three variables known as perceived severity, response efficacy, and perceived vulnerability. In 1983, Roger's initial PMT model was enhanced through collaboration with Maddux to include self-efficacy, highlighting two cognitive communication systems: threat evaluation and coping [40]. Protection motivation arises from both the threat appraisal and the coping appraisal. Threat appraisal refers to an individual's evaluation of the degree of peril presented by a menacing occurrence [41]. Meanwhile, The coping appraisal component of PMT pertains to an individual's evaluation of their capacity to manage and prevent probable loss or harm resulting from a danger [42] as cited in [43]. The Protection Motivation Theory (PMT) focuses on how individuals protect themselves from risks by considering the level of severity and vulnerability, this theory is also used to analyze security systems to prevent cyber-attacks [44]. For example, cybersecurity professionals might use the Protection Motivation Theory (PMT), which primarily explains how threat perception and self-efficacy influence security behaviors or attitudes within the population [40].

Perceived severity refers to the assessment of persons regarding the severity of consequences resulting from a danger [45]. A study by Alneyadi emphasized that perceived vulnerability and severity significantly affected users' intents to adopt AI-based cybersecurity systems, emphasizing the essential role these perceptions play in cybersecurity decision-making processes [39].

The original PMT proposed that individuals who perceive themselves as vulnerable to a threat will adopt measures to mitigate the risk [46]. Peng and Hwang's research emphasizes that perceptions of effectiveness and vulnerability significantly influence the adoption of e-learning technologies, suggesting that employees are more likely to engage with technology when they feel vulnerable to the consequences of not doing so [47].

Response efficacy refers to the extent to which an individual perceives that a advocated action would successfully alleviate their threat [48]. For example, Ling et al. demonstrated that perceived response efficacy is a unique predictor of intention, suggesting that when employees perceive that technology can significantly enhance their work processes, they are more likely to utilize it [49].

Self-efficacy is the conviction in one's capacity to accomplish a particular task [41], [50]. Self-efficacy was originally defined by Bandura as "the conviction that one can successfully execute the behavior required to produce outcomes" [51]. Rad et al. indicate that individuals with higher self-efficacy are more likely to engage in protective behaviors, suggesting that enhancing employees' confidence in their technological skills can lead to greater technology adoption [52].

2.4 Hypothesis Development

2.4.1 Perceived Ease of Use

The concept of PEOU is closely linked to user satisfaction and intention to use technology [53]. Research indicates that PEOU is a critical determinant of user attitudes toward adopting new technologies, including cybersecurity measures. For instance, Zhou et al. highlight that PEOU has a significant positive effect on perceived usefulness, which is crucial for fostering a favorable attitude toward adoption technology [54]. Furthermore, the role of user behavior and awareness cannot be overlooked. Moustafa et al. argue that user behavior significantly impacts cybersecurity management,

indicating that when users are aware of and understand the cybersecurity measures in place, their intention to comply and engage with these measures increases [55]. In this regard, it was hypothesized that:

H1: Perceived ease of use has a significant effect on the intention to use cybersecurity in client data security.

2.4.2 Perceived Usefulness

Perceived usefulness pertains to an individual's conviction about the degree to which the adoption of a new system might enhance their work performance, as stated in [33]. The perceived usefulness (PU) of cybersecurity measures significantly influences the intention to use these measures for client data security. This relationship is grounded in the Technology Acceptance Model (TAM), which asserts that perceived usefulness is a primary determinant of users' behavioral intentions towards adopting technology [56]. In the context of cybersecurity, when users perceive that security measures will enhance their ability to protect sensitive client data, their intention to utilize these measures increases. This is essential in environments where the collective intention to use cybersecurity measures can significantly enhance overall data security. For instance, when users find cybersecurity tools both useful and easy to use, their intention to adopt these tools is further strengthened [57]. In this regard, it was hypothesized that:

H2: Perceived usefulness has a significant effect on the intention to use cybersecurity in client data security.

2.4.3 Perceived Severity

Generally, when individuals recognise a threat, they frequently modify their behaviours based on the level of risk and assess their willingness to accept the threat [58]. Thus, [59]an individual's perceived severity tends to be positively linked to their intentions to follow protective actions. PMT posits that individuals with high perceptions of the severity of threats are more likely to comply with coping guidelines, a relationship confirmed by several information security studies, such as those by [60], which established that perceived severity significantly influences users' intentions to adhere to recommended guidelines. In this regard, it was hypothesized that:

H3: Perceived severity has a significant effect on the intention to use cybersecurity in client data security.

2.4.4 Perceived Vulnerability

Perceived vulnerability is one of the two threat appraisals in Protection Motivation Theory (PMT), denoting the extent to which an individual believes they are susceptible to a threat [41], [50]. The PMT indicates that an individual's perceived vulnerability is directly correlated with their intention to implement the suggested coping response. This suggests that users are inclined to adhere to the suggested security guidelines or additional security measures if they perceive a potential threat of attack [39]. Numerous studies have substantiated this correlation, particularly those aimed at identifying the determinants affecting the adoption of security technologies, including antivirus software [61], desktop security practices [62], and other innovations in information systems security [63]. Nevertheless, another study identified an indirect link between the two, with perceived threat serving as a mediating factor. Despite the varied findings that cast doubt on the application and significance of the PMT in information security research, it appears that the perceived susceptibility to cyber-attacks can substantially affect consumers' inclination to adopt cybersecurity systems [64]. In this regard, it was hypothesized that:

H4: Perceived vulnerability has a significant effect on the intention to use cybersecurity in client data security.

2.4.5 Perceived Response Efficacy

Response efficacy, which refers to the perceived effectiveness of a recommended coping mechanism in mitigating a threat, is an essential factor known to influence users' intentions to adopt technology, including information security systems [20], [62]. Evaluations of response efficacy are regarded as a cognitive process in which individuals assess the efficiency of a proposed solution in mitigating a threat [65] as cited in [66]. A substantial body of literature demonstrates that response efficacy is a critical factor of users' intention to adopt technology. In the study by [62],

response efficacy was identified as a principal factor influencing users' intentions to adhere to desktop security behaviours, while [66] recognised this variable as a crucial determinant of users' intentions to comply with security policies. Therefore, it was hypothesized that:

H5: Perceived response efficacy has a significant effect on the intention to use cybersecurity in client data security.

2.4.6 Perceived Self-Efficacy

Perceived self-efficacy plays a crucial role in influencing the intention to use cybersecurity measures for client information security. Self-efficacy, defined as an individual's belief in their capability to execute behaviors necessary to produce specific performance attainments, has been shown to significantly impact users' engagement with cybersecurity practices [67]. Findings from Sari et al., which highlighted that self-efficacy is a frequent factor influencing information security behavior, with numerous studies confirming its positive impact on users' intentions to engage in secure practices [67]. Moreover, Norisnita and Indriati, who confirmed that self-efficacy influences user intention and enhances trust in using new services, including cybersecurity tools [68]. Zhou et al. found positive associations between self-efficacy and secure behavior, indicating that individuals who feel capable of managing cybersecurity risks are more likely to engage in protective actions [69]. In this regard, it was hypothesized that:

H6: Perceived self-efficacy has a significant effect on the intention to use cybersecurity in client data security.

2.4.7 Moderating Effect of Gender

Throughout history studies have identified significant differences in attitudes, perceptions, and actions between men and women, highlighting the importance of gender in shaping beliefs, in familiarity with, attitudes towards, perceptions of, intentions to use, and adoption of information technologies [70], [71], [72], [73], [74]. Gender differences can significantly affect perceptions of technology, influencing both perceived usefulness (PU) and perceived ease of use (PEOU), which are critical components of TAM [75]. Research shows that women often perceive cybersecurity tools as more complicated and less useful than men do, which can hinder their adoption [76]. Similarly, Anwar et al., in the PMT framework, emphasize the importance of gender in threat assessment and coping mechanisms, as men and women show different responses to perceived cybersecurity risks and protective actions [77]. This framework collectively demonstrates how gender influences motivation, decision-making styles, and compliance behaviors, as evidenced by research highlighting gaps in self-efficacy, decision-making, and the adoption of protective behaviors [77], [78], [79]. These insights are crucial for developing targeted strategies that address gender-specific barriers, thereby promoting the broader adoption of cybersecurity measures across various user groups. In this regard, it was hypothesized that:

H7a: Gender moderates the relationship between perceived ease of use and the intention to adopt cybersecurity in client data security.

H7b: Gender moderates the relationship between perceived usefulness and the intention to adopt cybersecurity in client data security.

H7c: Gender moderates the relationship between perceived severity and the intention to adopt cybersecurity in client data security.

H7d: Gender moderates the relationship between perceived vulnerability and the intention to adopt cybersecurity in client data security.

H7e: Gender moderates the relationship between perceived response efficacy and the intention to adopt cybersecurity in client data security.
H7f: Gender moderates the relationship between perceived self-efficacy and the intention to adopt cybersecurity in client data security.

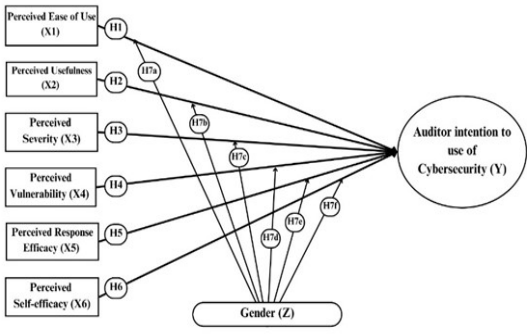

Figure 1. Research model

3. RESEARCH METHODOLOGY

3.1 Research Method

This study employs a quantitative methodology to examine the factors affecting auditors' intention to adopt cybersecurity, utilizing the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) frameworks. The quantitative approach is defined by the research and analysis of correlations among variables using gathered numerical data, subsequently employing statistical methods [80]. This research utilizes primary data collected through the distribution of questionnaires to respondents using Google Forms. The study employed questionnaires to gather respondents' personal data and indicators designed to evaluate the research variables. The participants in this study are auditors employed in Public Accounting Firms in Indonesia.

The employed sample approach is non-probability sampling, namely convenience sampling and snowball sampling. Convenience sampling is a method in which the researcher picks participants who are readily accessible or available during the study process. This method is frequently employed for its simplicity and effectiveness, particularly when time and affordability are primary considerations. This method is regarded as cost-effective and requires less effort relative to alternative sampling techniques [81]. Meanwhile, snowball sampling is a sampling technique where the initial respondents selected by the researcher are asked to recommend other individuals who have similar characteristics or are relevant to the study. This process continues indefinitely, causing the sample size to increase like a rolling snowball [82].

This research employs a methodology for an unknown population due to the fluctuating number of auditors at a public accounting company, as auditors may join or resign. The method used to determine the sample size follows Joseph Hair's, which states that for factor analysis, the ideal sample size is "a minimum of 5 to 10 respondents per indicator variable (item)" [83]. In this study, we applied the approach of using 10 times the number of indicators to determine the sample size. Consequently, it has been determined that the total number of responses will be 413.

This study will employ a six-point Likert scale, with 1 representing "strongly disagree' and 6 denoting 'strongly agree," to assess the variables of perceived ease of use, perceived usefulness, perceived severity, perceived vulnerability, response efficacy, and self-efficacy. The rationale for choosing a Likert scale of 1–6 is to eliminate the middle value. Kulas and Stachowski assert that respondents are inclined to select the middle value when it is available, this is influenced by Indecision or insufficient comprehension of the statement [84]. The score may exhibit bias if a significant number of respondents select the middle value. Gender will be indicated by two dummy variables, which differentiate between male and female. Respondents must express their degree of agreement with the questions on a Likert scale to prevent irrelevant responses. Researchers also employ the Likert scale to enhance data processing. This study employs statistical analysis for hypothesis testing. This study employs hypothesis testing using Structural Equation Modeling – Partial Least Square (SEM-PLS) using SmartPLS 4 software to analyze the gathered data.

3.2 Operation of Variables

The operationalization of variables aims to identify the indicators for measuring the variables in the research. Furthermore, the operationalization of variables is helpful in delineating the scale employed for each variable, hence aiding in the selection of suitable measuring instruments for hypothesis testing. Presented above is Table 1 for the operationalization of variables:

Table 1. Operation of Variables

Variable	Indicator	Source
Auditors' Perceived Ease of Use (PEOU)	1. Easy to learn. 2. Clear and understandable. 3. Working without any problems. 4. Easy to control technology. 5. Make the job easier. 6. Flexibility.	[26], [33], [37], [85]
Auditors' Perceived Usefulness (PU)	1. Improve my work. 2. Enhance my effectiveness. 3. Increase my productivity. 4. Makes work easier. 5. Job Performance. 6. Assessment of	[26], [33], [37], [86]

	benefit.	
Auditors' Perceived Severity (PS)	1. If clients suffered losing data because of cybersecurity incidents, it would be severe. 2. If clients suffered losing data because of cybersecurity incidents, it would be serious. 3. If clients suffered losing data because of cybersecurity incidents, it would be significant. 4. If client information were available to unauthorized users, it would be risky. 5. A security breach of client data would be a serious problem for the company. 6. I believe that protecting the information on my client is important.	[62], [87]
Auditors' Perceived Vulnerability (PV)	1. Clients are at risk of losing data by cybersecurity incidents. 2. It is likely that clients will lose data by cybersecurity incidents. 3. It is possible for clients to lose data by cybersecurity incidents. 4. My client could be subject to a serious information security threat. 5. My client is facing more and more information security threats. 6. My client could fall victim to a malicious attack if I fail to follow good cybersecurity practices.	[87], [88]
Auditors' Perceived Response Efficacy (PE)	1. Will work in solving cyber threat problems. 2. Effective in solving cyber threat problems. 3. Solving cyber threat problems is more likely to be guaranteed. 4. Enabling cyber security measures on client data will prevent security breaches. 5. The preventative measures available to stop people from getting confidential personal or financial information on client data are effective.	[87], [89]
Auditors' Perceived Self-efficacy (SE)	1. I believe that I would use cybersecurity to mitigate threats. 2. I feel confident that I would be able to operate cybersecurity to mitigate threats. 3. I feel confident with my ability, even without any guidelines on how to use it. 4. I feel comfortable taking measures to secure client data. 5. Taking the necessary cybersecurity measures is entirely under my control.	[87], [90]
Gender	1. Male 2. Female	[22]
Intention to use Cybersecurity in Client Data Security (ICS)	1. I intend to use it in the future. 2. I think I will always try to adopt. 3. I plan to use it frequently. 4. I am willing to fully adopt the cybersecurity system.	[22], [27]

4. RESEARCH RESULT AND DISCUSSION

4.1 Respondent Profile

For this study, a questionnaire was developed and distributed to a total of 429 respondents, all auditors employed by public accounting firms in Indonesia. After reviewing the responses, 16 outliers with overly fluctuating answers were excluded, leaving a final sample of 413 respondents. This sample size meets the minimum respondent requirement, following [91], which is at least five times the number of indicators used. The profile of respondents in this study includes the demographic characteristics of auditors who participated in the study on the adoption of

cybersecurity technology. The characteristics analyzed include gender, age, position, work experience, and the last level of education. Understanding these characteristics is important to provide an overview of the respondents' backgrounds and their potential influence on their intention to adopt cybersecurity technologies in audit practice. A summary of the respondents' identities is presented in the table below:

Table 2. Identity of Respondents

Characteristics	*N*	*%*
Gender		
Female	162	39.2%
Male	251	60.8%
Age		
20 - 30 years old	368	89.1%
31 - 40 years old	44	10.7%
41 - 50 years old	1	0.2%
Position		
Assistant Manager	26	6.3%
Associate	237	57.4%
Manager	7	1.7%
Senior Associate	143	34.6%
Experience		
1 - 5 years	339	82.1%
11 - 15 years	3	0.7%
6 - 10 years	71	17.2%
The highest level of education attained		
S1/D4	406	98.3%
S2	7	1.7%

The majority of respondents in this study were male (60.8%) and aged 20-30 years (89.1%), with the most positions as Associate (57.4%) and Senior Associate (34.6%). Most respondents have 1-5 years of work experience (82.1%) and the latest education level is S1/D4 (98.3%). This dominance of young auditors with relatively short work experience may affect their level of acceptance of the adoption of cybersecurity technology in audit practice.

4.2 Outer Loading Test

This test refers to the outer loading value which is used to assess the convergent validity of the indicators in the research model. According to [91], the recommended outer loading value is ≥ 0.7. However, indicators with loading values between 0.4 - 0.7 can be considered to be retained if the AVE value and composite reliability still meet the criteria. The results of the outer loading test are presented in Table 3 below.

Table 3. Outer Loading Value

Indicator	Loading
PEU1	0.927
PEU2	0.935
PEU3	0.913
PEU4	0.939
PEU5	0.914
PEU6	0.918
PU1	0.887
PU2	0.924
PU3	0.922
PU4	0.889
PU5	0.920
PU6	0.853
PS1	0.896
PS2	0.879
PS3	0.912
PS4	0.907
PS5	0.925
PS6	0.884
PV1	0.859
PV2	0.884
PV3	0.899
PV4	0.890
PV5	0.883
PV6	0.873
PE1	0.885
PE2	0.907
PE3	0.895
PE4	0.873
PE5	0.868
SE1	0.929
SE2	0.928
SE3	0.906

Indicator	Loading
SE4	0.938
SE5	0.921
ICS1	0.874
ICS2	0.894
ICS3	0.918
ICS4	0.886

Based on the outer loading test results, all indicators have a loading factor value above 0.5, even most of them are above 0.85. This shows that all indicators in the research model have strong convergent validity and are able to represent their constructs well. Thus, this model can be used for further analysis.

4.3 Validity and Reability Test

Validity in this study was tested using Average Variance Extracted (AVE), where an AVE value ≥ 0.50 indicates adequate convergent validity [91]. Reliability is tested with Composite Reliability (CR), where a CR value ≥ 0.70 indicates that the indicator can measure latent variables consistently. The results of validity and reliability tests are presented in Table 4 below.

Table 4. Composite Reliability and Average Variance Extracted

Variable	AVE	Composite reliability (rho_c)
PEU	0.855	0.972
PU	0.809	0.962
PS	0.811	0.963
PV	0.777	0.954
PE	0.784	0.948
SE	0.855	0.967
ICS	0.797	0.940

Based on the test results in Table 4, all variables have AVE values above 0.5 and composite reliability above 0.7. This shows that the research instruments meet the requirements of convergent validity and reliability, so they can be used in further analysis.

Discriminant validity testing aims to ensure that each construct in the model has a clear difference and there is no overlap between variables. One method used is the Fornell-Larcker Criterion, which compares the square root of the Average Variance Extracted (AVE) with the correlation between constructs. According to [91], discriminant validity is met if the square root of the AVE of a construct is greater than the correlation between other constructs. The Fornell-Larcker Criterion results are presented in Table 5 below.

Table 5. Fornell-Larcker Criterion

	PEU	PU	PS	PV	PE	SE	ICS
PEU	0.92						
PU	0.70	0.89					
PS	0.27	0.39	0.90				
PV	0.44	0.49	0.42	0.88			
PE	0.40	0.50	0.46	0.51	0.88		
SE	0.59	0.51	0.31	0.51	0.54	0.92	
ICS	0.29	0.38	0.39	0.27	0.50	0.47	0.89

Based on the results in Table 5, all constructs meet the Fornell-Larcker criteria, where the diagonal value is greater than the correlation between other variables. This indicates that each construct in the model has good discriminant validity and can be used for further analysis.

4.4 Coefficient of Determination Test

The coefficient of determination (R^2) is used to measure the extent to which the independent variable can explain the dependent variable in the model. According to [91], the R^2 value is categorized as substantial (≥ 0.75), moderate (≥ 0.50), and weak (≥ 0.25). The results of the *Coefficient of Determination Test* are presented in Table 6 below.

Table 6. Coefficient of Determination

	R-SQUARE	R-SQUARE ADJUSTED
ICS	0.359	0.349

Based on the results in Table 6, the R^2 value for the ICS variable is 0.359 with an adjusted R-square of 0.349. This indicates that the independent variables in the model are able to explain about 35.9% of the variation in ICS, while

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the rest is influenced by other factors outside the model. Thus, this model has a prediction level that is classified as weak to moderate.

4.5 Hypothesis Testing

Hypothesis testing is done with the bootstrapping technique in the PLS-SEM method. The hypothesis is considered significant if the T-statistic value > 1.96 at a significance level of 5% (p-value < 0.05) [91]. The results of direct hypothesis testing are presented in Table 7 below.

Table 7. Hypothesis Testing (Direct Effect)

Hypothesis	Original sample	T statistics	P values
H1: PEU ->ICS	-0.116	1.651	0.099
H2: PU -> ICS	0.150	2.304	0.021
H3: PS -> ICS	0.192	3.613	0.000
H4: PV -> ICS	-0.143	2.914	0.004
H5: PE -> ICS	0.277	5.044	0.000
H6: SE -> ICS	0.333	5.969	0.000

Based on the results in Table 6, hypotheses H2, H3, H4, H5, and H6 have a significant effect on ICS, as the T-statistic value is greater than 1.96 and the p-value < 0.05. Meanwhile, H1 (PEU -> ICS) is not significant (T-statistic = 1.651 and p-value = 0.099), which indicates that perceived ease of use does not have a significant direct impact on ICS. Thus, most of the hypotheses in this study can be accepted.

4.6 Hypothesis Testing (MGA)

Hypothesis testing using Multi-Group Analysis (MGA) is carried out with bootstrapping techniques in the Partial Least Squares method (PLS-SEM) to assess differences in relationships between latent variables based on groups (for example, gender: male vs. female). According to [91], the relationship difference is considered significant if the p-value < 0.05 in the PLS-MGA test. The results of the MGA test are presented in Table 8 below.

Table 8. Hypothesis Comparison Between Male and Female

Relationships	Males			Females		
	Original sample	T statistics	P values	Original sample	T statistics	P values
PEU ->ICS	-0.126	1.228	0.220	-0.084	0.750	0.453
PU -> ICS	0.213	2.385	0.017	0.020	0.208	0.835
PS -> ICS	0.164	2.243	0.025	0.240	2.930	0.003
PV -> ICS	-0.099	1.555	0.120	-0.175	2.041	0.041
PE -> ICS	0.227	3.020	0.003	0.354	4.445	0.000
SE -> ICS	0.313	5.113	0.000	0.348	3.191	0.001

Table 9. Hypothesis Testing for Gender

Hypothesis	Relationships	Differences (Male - Female)	p value (Male vs Female)	Remarks
H1a	PEU ->ICS	-0.042	0.772	Not supported
H2a	PU -> ICS	0.193	0.140	Not supported
H3a	PS -> ICS	-0.076	0.495	Not supported
H4a	PV -> ICS	0.076	0.472	Not supported
H5a	PE -> ICS	-0.127	0.242	Not supported
H6a	SE -> ICS	-0.035	0.775	Not supported

Based on the results in Table 8, the variables PU, PS, PE, and SE have a significant influence on ICS in the male group, while in the female group, the variables PS, PV, PE, and SE show a significant influence on ICS. However, the results of the between-groups difference test in

Table 9 show that there are no significant differences in the relationships between latent variables based on gender, as all p-values > 0.05. Thus, although there are differences in the relationships of the variables in each group, these differences are not statistically strong enough to be considered significant.

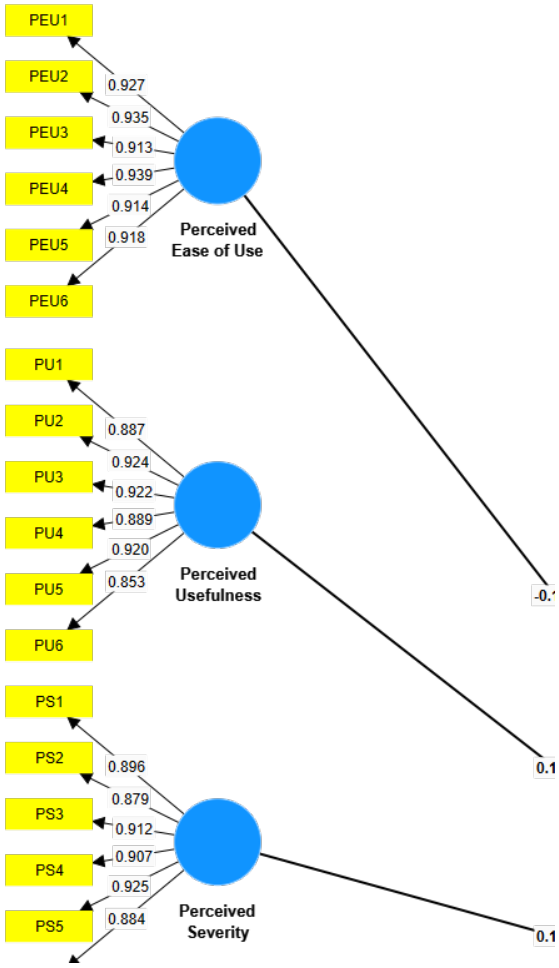

Figure 2. Research Path Coefficient

4.7 Discussion

Hypothesis 1, analysis of the effect of Perceived Ease of Use (PEU) on Auditor Intention to Use Cybersecurity shows that the ease of use factor of cybersecurity technology does not have a significant influence in encouraging auditors to adopt it. With a T-statistic value of 1.651 and a p-value of 0.099, as well as an original sample (O) of -0.116 indicating a negative relationship, this result shows that even though technology is easier to use, it does not necessarily increase auditors' intention to use it in their audit practice. This finding underscores that technology adoption in professional environments, particularly in auditing and cybersecurity, depends not only on ease-of-use factors but also on other more substantial factors, such as the tangible benefits that auditors derive from using technology. This result is in line with research conducted by [26], which found that Perceived Ease of Use has no direct influence on auditors' intention to use artificial intelligence-based technology in auditing. The study concluded that although an easier-to-use system can increase its perceived usefulness, ease of use does not automatically affect the auditor's decision to adopt it. Similarly, [92] found that ease of use only has a significant impact if it is supported by other factors, such as belief in the benefits of technology and individual readiness to adopt it. Meanwhile, research conducted by [93] confirms that in the field of auditing and cybersecurity, the effectiveness and efficiency of technology is prioritized over its convenience. Auditors are more likely to consider the extent to which technology can improve audit accuracy, speed, and effectiveness than whether the technology is easy to use.

Hypothesis 2, the results of statistical analysis show that Perceived Usefulness (PU) has a significant influence on Auditor Intention to Use Cybersecurity, with a T-statistic value of 2.304 and a p-value of 0.021. The original sample (O) value of 0.150 indicates a positive relationship, which indicates that the higher the auditors' perception of the benefits of cybersecurity technology, the greater their intention to adopt it in audit practice. This finding confirms that auditors who believe that these technologies can improve work efficiency and audit accuracy are more likely to use them than those who see less benefit from them. Auditors' perception of technology benefits plays a major role in their decision to adopt cybersecurity technology. Auditors who perceive that cybersecurity systems can improve the effectiveness of their work are more motivated to use them. Perceived benefits include increased efficiency in threat identification, accelerated audit processes, and increased accuracy in audit data processing. This suggests that auditors are more likely to adopt technologies that are proven to add value to their work, rather than simply considering the easier aspects of use. This finding is in line with previous research, such as that conducted by [26], which found that Perceived Usefulness has a significant influence on auditors' intention to adopt Machine Learning in auditing. The study shows that auditors who see real benefits

from technology are more likely to use it in their work. In addition, research by [27] on Internet of Things (IoT) adoption in remote auditing also found that Perceived Usefulness is a major factor in auditors' decision to use new technology in auditing. These two studies reinforce the finding that the tangible benefits of technology are the main driving factor in technology adoption in auditing. In addition, [56] also confirmed that the human factor in the decision to adopt cybersecurity technology in the health sector is highly dependent on the perceived benefits of the technology.

Hypothesis 3, the results of statistical analysis show that Perceived Severity (PS) has a significant influence on auditors' intention to use cybersecurity technology, with a T-statistic of 3.613 and a p-value of 0.000. The original sample (O) value of 0.192 indicates that the higher the auditors' perception of the severity of cyber threats, the greater their propensity to adopt cybersecurity technology in their work. This finding confirms that awareness of the negative consequences of cyber threats is a major factor in encouraging auditors to adopt cybersecurity systems. Auditors who understand that cyberattacks can lead to data leaks, financial losses, and decreased organizational credibility will be more motivated to implement stricter security measures. Therefore, perceptions of the risks and negative impacts of cyberattacks play a major role in driving auditors' decisions to adopt cybersecurity technology. This finding is in line with previous research, such as that conducted by [94], which found that Perceived Severity has a significant impact on individuals' intention to use digital-based security alert systems. The higher an individual's perception of the danger posed by cyber threats, the higher their motivation to adopt security technology. In addition, research by [47] also confirmed that Perceived Severity plays an important role in driving the adoption of digital security-based e-learning systems, where individuals who are aware of potential security threats are more likely to use systems designed to protect their data.

Hypothesis 4, the results of statistical analysis show that Perceived Vulnerability (PV) has a significant influence on auditors' intention to use cybersecurity technology, with a T-statistic of 2.914 and a p-value of 0.004. The original sample (O) value of -0.143 indicates that the higher the auditors' perception of their likelihood of being exposed to cyber threats, the greater their tendency to adopt cybersecurity technology in their audit practice. Auditors who feel their systems are vulnerable to hacker attacks, data theft, or malware will be more encouraged to implement security technologies to mitigate these risks. Factors that influence this perception of vulnerability include direct experience with security incidents, information on the latest threats, and compliance with data protection regulations. Given the increase in cyberattacks targeting financial and audit institutions, auditors with high perceptions of their vulnerability will be more motivated to use more sophisticated and effective digital protection systems. This finding is also supported by [61] research, which found that Perceived Vulnerability plays a role in increasing individuals' awareness of cybersecurity risks and encouraging them to adopt protective measures. The study shows that individuals who feel more vulnerable to cyberattacks tend to be more proactive in implementing stricter digital security practices to reduce potential threats. In addition, [39] study emphasized that organizational support and strict regulations play a role in strengthening the relationship between perceived vulnerability and the use of cybersecurity technologies, especially in the audit and finance sectors. Clear regulations and strict security policies can increase individuals' sense of urgency in adopting better protection systems. Therefore, increased awareness of potential threats and strong regulatory support are key factors in driving the adoption of cybersecurity technologies in professional environments.

Hypothesis 5, the results of statistical analysis show that Perceived Response Efficacy (PE) has a significant influence on auditors' intention to adopt cybersecurity technology. The T-statistic value of 5.044 and p-value of 0.000 confirm this significant relationship. In addition, the original sample (O) value of 0.277 indicates that the higher the auditors' perception of the effectiveness of cybersecurity measures in preventing or mitigating cyber threats, the greater their propensity to use them in the audit process. Auditors who believe that cybersecurity systems can provide effective protection are more likely to adopt these technologies to ensure the security of audit data and information. Auditors' confidence in the effectiveness of cybersecurity systems plays a major role in their decision to adopt them. Auditors who believe that cybersecurity technology can prevent data leakage, protect client information, and detect threats quickly and accurately will be more encouraged to use it. The more confident the system is in providing protection, the more likely

auditors are to adopt it in their audit practice. This finding is in line with the research of [95], which found that Perceived Response Efficacy has a significant influence on cybersecurity behavior among government employees. This study shows that individuals who have high confidence in the effectiveness of the protection system tend to be more disciplined in implementing digital security measures to reduce the risk of cyber attacks. Then in [96] research, it explains that Perceived Response Efficacy has a significant influence on individual motivation in accessing protection information in the future, which means that there is a significant influence of Perceived Response Efficacy on information intentions. In addition, [97]confirms that users who feel that cybersecurity systems can reduce threats are more likely to actively adopt these technologies, especially in the financial and audit sectors. This study indicates that individuals who believe that the security measures they take are truly effective in reducing threats are more likely to implement cyber protection measures consistently.

Hypothesis 6, the results of statistical analysis show that Perceived Self-Efficacy has a significant effect on auditors' intention to adopt cybersecurity technology. The T-statistic value of 5.969 and p-value of 0.000 confirm this significant relationship. In addition, the original sample (O) value of 0.333 indicates that the higher auditors' confidence in their ability to use cybersecurity technology, the more likely they are to implement it in audit practice. Auditors who have high self-efficacy in understanding, managing, and implementing cybersecurity systems are more prepared and motivated to use them in their work. In contrast, auditors with low self-efficacy may experience hesitation in adopting these technologies, even though they recognize their benefits. The main factors that can increase auditor self-efficacy include previous experience in using technology, adequate training, and organizational support. [47] research shows that self-efficacy plays a major role in users' decisions to adopt digital security technologies, especially in systems that require high levels of technical skills. Individuals with higher levels of self-efficacy tend to be more confident in using and implementing digital security technologies. Support for this finding was also found in [98] and [99] study, which found that computer self-efficacy has a significant positive effect on the intention to use CAATs. This study shows that individuals with higher levels of computer self-efficacy tend to have greater confidence in operating technology, thus increasing the likelihood of adopting the technology. This indicates that individuals' belief in their ability to use technology plays an important role in shaping their intention to use it. Thus, the higher a person's level of computer self-efficacy, the more likely they are to adopt and utilize technology effectively in their work environment.

Hypothesis 7a, the results showed that Perceived Ease of Use (PEU) did not have a significant influence on Intention to Use Cybersecurity (ICS) in both men ($b = -0.126$, $p > 0.05$) and women ($b = -0.084$, $p > 0.05$), with differences between groups also not significant ($b = -0.042$, $p > 0.05$). This indicates that ease of use is not a major factor in the adoption of cybersecurity technology, regardless of user gender. The absence of a significant moderating effect of gender suggests that both men and women have similar barriers in the ease of use aspect of cybersecurity technology. Research by [76] found that women tend to see technology as more complex and less useful than men, which may hinder the adoption of cyber technology. In this case, differences in perceived ease of use between men and women may affect how they interact with cybersecurity technologies. In addition, [77] asserted that in the context of cybersecurity, men are more confident in assessing the ease of use of systems than women, who often feel less familiar with advanced technologies.

Hypothesis 7b, the results showed that Perceived Usefulness (PU) has a significant influence on Intention to Use Cybersecurity (ICS) in men ($b = 0.213$, $p < 0.05$) but not in women ($b = 0.020$, $p > 0.05$). However, the difference between the two groups was not significant ($b = 0.193$, $p > 0.05$), indicating that gender did not moderate the relationship between PU and ICS. This suggests that while technology usability is an important factor for men, other factors may be more influential in women's decision to adopt cybersecurity. These findings suggest that men are more likely to adopt cybersecurity technology if they see direct benefits in improving work efficiency and data protection. This is in line with [79] research, which found that men focus more on the functional aspects of technology and how much technology can provide direct benefits in their work. In contrast, women may consider other factors such as trust in the system and social support in technology adoption decisions. The study of [78] supports this finding by showing that

women are more influenced by external factors, including the social environment and organizational policies, in making decisions regarding the adoption of cybersecurity technology. However, the absence of significant differences between men and women in the relationship between Perceived Usefulness and adoption intention suggests that technology benefits remain an important factor for both genders, but with different weights of consideration. While men focus more on efficiency and performance, women may consider more aspects of security, trust, and ease of implementation in the work environment.

Hypothesis 7c, the results showed that the relationship between Perceived Severity (PS) and Intention to Use Cybersecurity (ICS) was significant for both men ($b = 0.164$, $p < 0.05$) and women ($b = 0.240$, $p < 0.05$). However, the difference between the two groups was not significant ($b = -0.076$, $p > 0.05$), indicating that gender did not moderate the relationship between PS and ICS. This suggests that perceptions of cyber threat severity affect cybersecurity technology adoption decisions similarly in both genders. These findings suggest that both men and women understand the importance of protection against cyber threats, and their awareness of potential risks drives decisions to adopt security measures. The study by [100] found that although there were significant differences in security and privacy behaviors between men and women, these differences were not large enough to cause significant moderating effects in the adoption of security technologies. The results showed that women tend to have a higher level of security awareness than men. However, although there is no significant difference between men and women in terms of the impact of Perceived Severity on adoption intentions, some previous studies have found that men are more likely to take technical solution-based measures, whereas women are more likely to rely on policy-based mitigation strategies and regulatory compliance [77].

Hypothesis 7d, the results showed that Perceived Vulnerability (PV) was not significant for men ($b = -0.099$, $p > 0.05$) but significant for women ($b = -0.175$, $p < 0.05$). However, the difference between the two groups was not significant ($b = 0.076$, $p > 0.05$), indicating that gender did not moderate the relationship between PV and Intention to Use Cybersecurity (ICS). This suggests that men are more sensitive to their perceived vulnerability to cyber threats than women, but overall gender does not act as a moderator in this relationship. This suggests that increased awareness of cyber risks and protection strategies should be targeted to all users, regardless of gender. The results of this study indicate that men are more likely to consider vulnerability factors in their decision to adopt cybersecurity technology than women. This finding contradicts some previous studies, such as the one conducted by [78], who found that women are more wary of digital security risks due to their higher concern for privacy and personal data protection than men. Likewise, the study by [77] confirmed that women often have a higher level of risk awareness in the context of information security, which may increase their likelihood of adopting protective measures.

Hypothesis 7e, the results showed that Perceived Response Efficacy (PE) has a significant influence on Intention to Use Cybersecurity (ICS) for both men ($b = 0.227$, $p < 0.05$) and women ($b = 0.354$, $p < 0.05$). However, the difference between groups was not significant ($b = -0.127$, $p > 0.05$), indicating that gender did not moderate the relationship between PE and ICS. This suggests that perceived response efficacy cybersecurity plays an important role in technology adoption decisions, without significant differences between genders. This finding indicates that both men and women see the effectiveness of cybersecurity systems as a key factor in their decision to adopt them. In other words, individuals tend to be more motivated to use cybersecurity technology if they believe that the system is truly capable of protecting data and mitigating cyber threats. [79] research found that the effectiveness of cybersecurity systems was rated similarly by men and women, so there is no significant moderating effect in the adoption of these technologies. However, although there is no significant moderating difference, some previous studies suggest that men and women may have different reasons for assessing the effectiveness of a security system. Men tend to focus more on technical aspects and system performance, while women consider reliability and ease of implementation in their daily work context [77]. Therefore, although the effect of Perceived Response Efficacy on technology adoption intention is similar for both genders, communication and training approaches can be adjusted to improve the effectiveness of adoption strategies.

Hypothesis 7f, the results showed that Self-Efficacy (SE) has a significant influence on

Intention to Use Cybersecurity (ICS) for both men ($b = 0.313$, $p < 0.05$) and women ($b = 0.348$, $p < 0.05$). However, the difference between the two groups was not significant ($b = -0.035$, $p > 0.05$), indicating that gender did not moderate the relationship between SE and ICS. This suggests that confidence in using cybersecurity technology is an important factor in technology adoption, regardless of the user's gender. The results of this study indicate that Self-Efficacy has a significant influence on auditors' intention to use cybersecurity technology, both in men and women. This finding is consistent with the study of [77], which asserts that although there are gender differences in confidence in technology, these differences are not large enough to be a significant moderating factor in the adoption of cybersecurity systems. That is, both men and women are likely to adopt cybersecurity technologies if they feel confident enough in using them. However, although there is no significant moderating effect, some studies suggest that women tend to experience higher psychological barriers in dealing with new technologies than men [78]. Therefore, although Self-Efficacy generally plays an important role in technology adoption decisions, organizations may need to consider more inclusive training strategies to ensure that all users have a sufficient level of confidence in using cybersecurity systems.

5. CONCLUSION

The results of this study indicate that factors in the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) such as Perceived Usefulness, Perceived Severity, Perceived Vulnerability, Perceived Response Efficacy, and Perceived Self-Efficacy have a significant influence on auditors' intention to adopt cybersecurity technology. However, Perceived Ease of Use does not have a significant influence in encouraging auditors to use cybersecurity technology. In addition, gender does not moderate the relationship between these factors and auditors' intention to use cybersecurity technology. This finding indicates that although there are differences in perceptions between men and women in assessing technology, these differences are not large enough to be a significant moderating factor in cybersecurity technology adoption decisions. This suggests that cybersecurity technology implementation strategies can be applied generally without the need for differentiation based on gender.

This research contributes to the strengthening of the TAM and PMT models in the context of cybersecurity technology adoption by auditors. The results of this study support previous findings that factors such as technology benefits, threat perception, and belief in protection effectiveness play an important role in the adoption of cybersecurity technology. However, they also challenge the assumption that gender moderates the relationship between these factors and cybersecurity technology adoption intentions. In addition, this study expands the understanding of how auditors, both male and female, make decisions in adopting cybersecurity technologies. In the absence of significant moderating effects, this study emphasizes the importance of internal factors such as confidence in technology use (Self-Efficacy) over demographic factors such as gender.

The findings of this study have several implications for audit organizations and policymakers in increasing the adoption of cybersecurity technologies. Organizations should provide training that emphasizes the tangible benefits of cybersecurity technologies in improving auditors' work efficiency. In addition, providing easily accessible technical support will help auditors be more confident in using cybersecurity systems. Awareness campaigns that educate auditors about cyber threats and effective protection measures can increase their understanding of the importance of cybersecurity technology adoption. Since gender does not moderate the relationship in this model, cybersecurity technology implementation strategies should be designed to reach all auditors equally without the need for different gender-based approaches.

While this study provides valuable insights, there are some limitations that need to be noted. This study only focuses on gender moderation, while other factors such as technology experience or organizational culture may moderate the relationship in this model. In addition, the sample of this study only consists of auditors in Indonesia, so generalization to the global context still needs to be further studied. The survey-based research method used in this study may not fully capture the more complex psychological dynamics related to cybersecurity technology adoption.

Based on the limitations that have been identified, some suggestions for future research are to adopt a mixed-method approach by adding in-depth interviews or case studies to gain a more comprehensive understanding of the psychological

factors that influence the adoption of cybersecurity technology. In addition, future research could expand the sample coverage to include auditors from different countries or other industry sectors to test whether the results of this study are consistent in various contexts. Further research can also consider other factors such as the level of technology experience of auditors or the influence of organizational culture in the adoption of cybersecurity systems. With more comprehensive follow-up research, it is hoped that a deeper understanding of the factors that influence auditors' adoption of cybersecurity technology and the best strategies to improve the implementation of cybersecurity systems in the audit profession can be obtained.

REFERENCES

[1] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, pp. 1–20, 2023, doi: 10.3390/s23156666.

[2] I. Munoko, H. L. Brown-Liburd, and M. Vasarhelyi, "The Ethical Implications of Using Artificial Intelligence in Auditing," *J. Bus. Ethics*, vol. 167, no. 2, pp. 209–234, 2020, doi: 10.1007/s10551-019-04407-1.

[3] PWC, "The C-suite playbook: Putting security at the epicenter of innovation," 2023. [Online]. Available: https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/pwc-2024-global-digital-trust-insights.pdf

[4] PWC, "Cloud-related threats are among the top three cyber concerns for 51% of Asia Pacific organisations over the next 12 months, according to PwC's Digital Trust Insights Asia Pacific 2024." Accessed: Nov. 05, 2024. [Online]. Available: https://www.pwc.com/id/en/media-centre/press-release/2024/english/digital-trust-insights-asia-pacific-2024.html

[5] PWC, "94% of investors believe corporate reporting on sustainability performance contains unsupported claims: PwC 2023 Global Investor Survey." Accessed: Oct. 16, 2024. [Online]. Available: https://www.pwc.com/gx/en/news-room/press-releases/2023/pwc-2023-global-investor-survey.html

[6] OJK, "Ketahanan dan Keamanan Siber Bagi Bank Umum." Accessed: Nov. 05, 2024. [Online]. Available: https://ojk.go.id/id/regulasi/Pages/Ketahanan-dan-Keamanan-Siber-Bagi-Bank-Umum.aspx

[7] S. V. Tritama, N. A. Mahaprajna, and B. L. Handoko, "the Role of Ai Adoption in Achieving Sustainable Audit Quality," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 2, pp. 547–561, 2025.

[8] T. G. Calderon and L. Gao, "Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees," *Int. J. Audit.*, vol. 25, no. 1, pp. 24–39, 2021, doi: 10.1111/ijau.12209.

[9] E. Raguseo, "Big data technologies: An empirical investigation on their adoption, benefits and risks for companies," *Int. J. Inf. Manage.*, vol. 38, no. 1, pp. 187–195, 2018, doi: 10.1016/j.ijinfomgt.2017.07.008.

[10] P. Rosati, F. Gogolin, and T. Lynn, "Audit Firm Assessments of Cyber-Security Risk: Evidence From Audit Fees and SEC Comment Letters," *Int. J. Account.*, vol. 54, no. 03, p. 1950013, 2019, doi: 10.1142/s1094406019500136.

[11] U. Ani, H. He, and A. Tiwari, "Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure," pp. 169–182, 2016, doi: 10.1007/978-3-319-41932-9_14.

[12] T. V. Eaton, J. H. Grenier, and D. Layman, "Accounting and cybersecurity risk management," *Curr. Issues Audit.*, vol. 13, no. 2, pp. C1–C9, 2019, doi: 10.2308/ciia-52419.

[13] M. F. Almufareh and M. Humayun, "Improving the Safety and Security of Software Systems by Mediating SAP Verification," *Appl. Sci.*, vol. 13(1), p. 647, 2023, doi: 10.4324/9781315232140-14.

[14] M. Eulerich, A. Masli, J. Pickerd, and D. A. Wood, "The Impact of Audit Technology on Audit Task Outcomes: Evidence for Technology-Based Audit Techniques*," *Contemp. Account. Res.*, vol. 40, no. 2, pp. 981–1012, 2023, doi: 10.1111/1911-3846.12847.

[15] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, no. 10, pp. 13–21, 2014, doi: 10.22215/timreview835.

[16] M. Anwar, W. He, I. K. Ash, X. Yuan, L. Li, and L. D. Xu, "Gender Difference and Employees' Cybersecurity Behaviors," *Comput. Human Behav.*, vol. 69, pp. 437–443, 2017, doi: 10.1016/j.chb.2016.12.040.

[17] D. Calisir, F., Gumussoy, C., Bayraktaroglu, A., & Karaali, "Predicting the intention to use a

web-based learning system:," *Hum. Factors Ergon. Manuf. Serv. Ind.*, vol. 24, no. 5, pp. 515–531, 2014, doi: 10.1002/hfm.

[18] V. Venkatesh and F. Davis, "A theoretical extension of the tecgnology acceptance model: Four longitudinal field studies University of Maryland at College Park," *Manage. Sci.*, vol. 46, no. 2, pp. 186–204, 2000.

[19] P. A. Rippetoe and R. W. Rogers, "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping With a Health Threat," *J. Pers. Soc. Psychol.*, vol. 52, no. 3, pp. 596–604, 1987, doi: 10.1037/0022-3514.52.3.596.

[20] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975, doi: 10.1080/00223980.1975.9915803.

[21] S. L. Bem, "Gender schema theory: A cognitive account of sex typing," *Psychol. Rev.*, vol. 88, no. 4, pp. 354–364, 1981, doi: 10.1037/0033-295X.88.4.354.

[22] A. Mahmud, M. N. Yusoff, and M. H. Husin, "Generation Z's adoption of IoT: protection motivation theory as the underlying model and gender as a moderator," *J. Syst. Inf. Technol.*, vol. 25, no. 2, pp. 133–159, 2023, doi: 10.1108/JSIT-02-2022-0054.

[23] C. S. Lee and Y. T. Chua, "The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States," *Crime Delinq.*, vol. 70, no. 9, pp. 2250–2277, 2023, doi: 10.1177/00111287231180093.

[24] J. Addae, X. Sun, D. Towey, and M. Radenkovic, "Exploring User Behavioral Data for Adaptive Cybersecurity," *User Model. User-adapt. Interact.*, vol. 29, no. 3, pp. 701–750, 2019, doi: 10.1007/s11257-019-09236-5.

[25] H. Gangwar, H. Date, and R. Ramaswamy, "Understanding determinants of cloud computing adoption using an integrated TAM-TOE model," *J. Enterp. Inf. Manag.*, vol. 28, no. 1, pp. 107–130, 2015, doi: 10.1108/JEIM-08-2013-0065.

[26] B. L. Handoko, D. S. Indrawati, and S. R. P. Zulkarnaen, "Embracing AI in Auditing: An Examination of Auditor Readiness Through the TRAM Framework," *Int. J. Comput. Methods Exp. Meas.*, vol. 12, no. 1, pp. 53–60, 2024, doi: 10.18280/ijcmem.120106.

[27] N. P. Maharani, C. R. Salim, and B. L. Handoko, "Internet of Things (Iot) Adoption in Remote Audit: a Quantitative Study Applying the Technology Acceptance Model," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 6, pp. 2480–2492, 2024.

[28] N. Z. Iskandar, William, and K. Deniswara, "Toward Secure Auditing: a Study on Auditor Readiness in Cybersecurity Implementation Using Extended Utaut Frameworks," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 4, pp. 1179–1188, 2025.

[29] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Inf. Fusion*, vol. 97, no. March, 2023, doi: 10.1016/j.inffus.2023.101804.

[30] F. Alharbi *et al.*, "The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia," *Sensors*, vol. 21, no. 20, 2021, doi: 10.3390/s21206901.

[31] C. Low, Y. Chen, and M. Wu, "Understanding the determinants of cloud computing adoption," *Ind. Manag. Data Syst.*, vol. 111, no. 7, pp. 1006–1023, 2011, doi: 10.1108/02635571111161262.

[32] H. O. Awa, O. U. Ojiabo, and B. C. Emecheta, "Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs," *J. Sci. Technol. Policy Manag.*, vol. 6, no. 1, pp. 76–94, 2015, doi: 10.1108/JSTPM-04-2014-0012.

[33] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q. Manag. Inf. Syst.*, vol. 13, no. 3, pp. 319–339, 1989, doi: 10.2307/249008.

[34] Z. Kevin, L. K. Kenneth, and X. Sean, "Electronic Business Adoption by European Firms: A Cross- country Assessment of the Facilitators and Inhibitors," *Eur. J. Inf. Syst.*, vol. 12, no. 4, pp. 251–268, 2003.

[35] F. Kolini and L. Janczewski, "Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review," *Commun. Assoc. Inf. Syst.*, vol. 50, no. 1, pp. 86–121, 2022, doi: 10.17705/1CAIS.05004.

[36] J. D. Bryan and T. Zuva, "A Review on TAM and TOE Framework Progression and How These Models Integrate," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 6, no. 3, pp. 137–145, 2021, doi: 10.25046/aj060316.

[37] V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decis. Sci.*, vol. 39, no. 2, pp. 273–315, 2008, doi: 10.1111/j.1540-

5915.2008.00192.x.
[38] N. Thi *et al.*, "The Effect of Technology Readiness on Adopting Artificial Intelligence in Accounting and Auditing in Vietnam," 2024.
[39] M. R. M. Al Humaid Alneyadi and M. K. Normalini, "Factors Influencing User'S Intention To Adopt Ai-Based Cybersecurity Systems in the Uae," *Interdiscip. J. Information, Knowledge, Manag.*, vol. 18, pp. 459–486, 2023, doi: 10.28945/5166.
[40] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983, doi: 10.1016/0022-1031(83)90023-9.
[41] R. Rogers W., "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation," *Soc. Psychophysiol. A Sourceb.*, no. October, pp. 153–177, 1983.
[42] P. Sychodynamic, "TO, A PROTECTION MOTIVATION THEORY APPROACH SECURITY, HOME WIRELESS," vol. 5, pp. 186–204, 2013.
[43] P. Ifinedo, "Understanding Information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, no. 31, pp. 83–95., 2012.
[44] A. C. Clubb and J. C. Hinkle, "Protection motivation theory as a theoretical framework for understanding the use of protective measures," *Crim. Justice Stud.*, vol. 28, no. 3, pp. 336–355, 2015, doi: 10.1080/1478601X.2015.1050590.
[45] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Comput. Human Behav.*, vol. 28, no. 6, pp. 2366–2375, 2012, doi: 10.1016/j.chb.2012.07.008.
[46] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu, "Health information privacy concerns, antecedents, and information disclosure intention in online health communities," *Inf. Manag.*, vol. 55, no. 4, pp. 482–493, 2018, doi: 10.1016/j.im.2017.11.003.
[47] M. H. Peng and H. G. Hwang, "An empirical study to explore the adoption of e-learning social media platform in taiwan: An integrated conceptual adoption framework based on technology acceptance model and technology threat avoidance theory," *Sustain.*, vol. 13, no. 17, 2021, doi: 10.3390/su13179946.
[48] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manage.*, vol. 45, no. February 2018, pp. 13–24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.
[49] B. A. Ling, M., Kothe, E. J., & Mullan, "Predicting intention to receive a seasonal influenza vaccination using Protection Motivation Theory," *Soc. Sci. Med.*, vol. 233, pp. 87–92, 2019.
[50] C. Y. Huang and Y. S. Kao, "UTAUT2 Based Predictions of Factors Influencing the Technology Acceptance of Phablets by DNP," *Math. Probl. Eng.*, vol. 2015, 2015, doi: 10.1155/2015/603747.
[51] A. Bandura, Bandura A, and A. Bandura, "Bandura 1977.pdf," 2006.
[52] R. E. Rad *et al.*, "Application of the Protection Motivation Theory for Predicting COVID-19 Preventive Behaviors in Hormozgan, Iran: A Cross-Sectional Study," *BMC Public Health*, vol. 21, no. 1, 2021, doi: 10.1186/s12889-021-10500-w.
[53] A. Mishra, A. Shukla, N. P. Rana, W. L. Currie, and Y. K. Dwivedi, "Re-examining post-acceptance model of information systems continuance: A revised theoretical model using MASEM approach," *Int. J. Inf. Manage.*, vol. 68, no. August 2022, p. 102571, 2023, doi: 10.1016/j.ijinfomgt.2022.102571.
[54] H. Zhou, J. Liu, and X. Cui, "Research on Influencing Factors of Adoption Behavior of Mobile Readers Based on Meta-Analysis," *Math. Probl. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/5082594.
[55] A. A. Moustafa, A. Bello, and A. Maurushat, "The Role of User Behaviour in Improving Cyber Security Management," *Front. Psychol.*, vol. 12, no. June, pp. 1–9, 2021, doi: 10.3389/fpsyg.2021.561011.
[56] S. Nifakos *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sensors*, vol. 21, no. 15, pp. 1–25, 2021, doi: 10.3390/s21155119.
[57] M. Kianpour, H. Øverby, S. J. Kowalski, and C. Frantz, "Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11594 LNCS, pp. 149–163, 2019, doi: 10.1007/978-3-030-22351-9_10.
[58] M. Workman, W. H. Bommer, and D. Straub,

"Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008, doi: 10.1016/j.chb.2008.04.005.

[59] C. Pechmann, G. Zhao, M. E. Goldberg, and E. T. Reibling, "What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes," *J. Mark.*, vol. 67, no. 2, pp. 1–18, 2003, doi: 10.1509/jmkg.67.2.1.18607.

[60] T. S. Wong, A. Gaston, S. DeJesus, and H. Prapavessis, "The utility of a protection motivation theory framework for understanding sedentary behavior," *Heal. Psychol. Behav. Med.*, vol. 4, no. 1, pp. 29–48, 2016, doi: 10.1080/21642850.2015.1128333.

[61] S. M. Debb and M. K. Mcclellan, "Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior," *Cyberpsychology, Behav. Soc. Netw.*, vol. 24, no. 9, pp. 605–611, 2021, doi: 10.1089/cyber.2021.0043.

[62] B. Hanus and Y. "Andy" Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 2–16, 2016, doi: 10.1080/10580530.2015.1117842.

[63] S. N. Suhaimi, N. F. Othman, R. Syahirah, S. Anawar, Z. Ayop, and C. F. M. Foozy, "Determinants of Privacy Protection Behavior in Social Networking Sites," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, pp. 285–292, 2020, doi: 10.14569/IJACSA.2020.0111236.

[64] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010, doi: 10.17705/1jais.00232.

[65] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," 1992. doi: 10.1080/03637759209376276.

[66] A. C. Johnston and M. Warkentin, "Fear appeals and information s ecurity behaviors: An empirical study," *MIS Q. Manag. Inf. Syst.*, vol. 34, no. SPEC. ISSUE 3, pp. 549–566, 2010, doi: 10.2307/25750691.

[67] P. K. Sari, P. W. Handayani, A. N. Hidayanto, S. Yazid, and R. F. Aji, "Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors," *Healthc.*, vol. 10, no. 12, 2022, doi: 10.3390/healthcare10122531.

[68] M. Norisnita and F. Indriati, "Application of Theory of Planned Behavior (TPB) in Cryptocurrency Investment Prediction: A Literature Review," *J. Econ. Bus.*, vol. 5, no. 2, 2022, doi: 10.31014/aior.1992.05.02.424.

[69] G. Zhou, M. Gou, Y. Gan, and R. Schwarzer, "Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage," *Front. Psychol.*, vol. 11, no. June, pp. 1–8, 2020, doi: 10.3389/fpsyg.2020.01066.

[70] Z. Cai, X. Fan, and J. Du, "Gender and attitudes toward technology use: A meta-analysis," *Comput. Educ.*, vol. 105, pp. 1–13, 2017, doi: 10.1016/j.compedu.2016.11.003.

[71] I. Janssen Reinen and T. Plomp, "Information technology and gender equality: A contradiction in terminis?," *Comput. Educ.*, vol. 28, no. 2, pp. 65–78, 1997, doi: 10.1016/s0360-1315(97)00005-5.

[72] C. S. Ong and J. Y. Lai, "Gender differences in perceptions and relationships among dominants of e-learning acceptance," *Comput. Human Behav.*, vol. 22, no. 5, pp. 816–829, 2006, doi: 10.1016/j.chb.2004.03.006.

[73] P. Schumacher and J. Morahan-Martin, "Gender, Internet and computer attitudes and experiences," *Comput. Human Behav.*, vol. 17, no. 1, pp. 95–110, 2001, doi: 10.1016/S0747-5632(00)00032-7.

[74] G. Torkzadeh and T. P. Van Dyke, "Effects of training on Internet self-efficacy and computer user attitudes," *Comput. Human Behav.*, vol. 18, no. 5, pp. 479–494, 2002, doi: 10.1016/S0747-5632(02)00010-9.

[75] P. Dutta and A. S. Borah, "A Study on Role of Moderating Variables in Influencing Employees' Acceptance of Information Technology," *Vision*, vol. 22, no. 4, pp. 387–394, 2018, doi: 10.1177/0972262918803467.

[76] B. Zhang, K. Ali, and T. Kanesan, "A Model of Extended Technology Acceptance for Behavioral Intention Toward EVs With Gender as a Moderator," *Front. Psychol.*, vol. 13, 2022, doi: 10.3389/fpsyg.2022.1080414.

[77] A. Kovačević, N. Putnik, and O. Tošković, "Factors Related to Cyber Security Behavior," *Ieee Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/access.2020.3007867.

[78] A. Duzenci, H. Kitapçı, and M. Ş. Gök, "The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior," *Appl. Sci.*, vol. 13, no. 15, p. 8731, 2023, doi: 10.3390/app13158731.

[79] D. V Tran, "Exploring the Influence of

Government Social Media on Cybersecurity Compliance: Employee Attitudes, Motivation and Behaviors," *J. Asia Bus. Stud.*, vol. 18, no. 1, pp. 204–223, 2023, doi: 10.1108/jabs-09-2023-0343.

[80] J. D. Creswell, J. W., & Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches.*, 4th ed. Thousand Oaks, CA: Sage publications, 2014.

[81] J. Golzar and S. Noor, "Defining Convenience Sampling in a Scientific Research," *Int. J. Educ. Lang. Stud.*, vol. 1, no. November, pp. 72–77, 2022.

[82] J. Kirchherr and K. Charles, "Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia," *PLoS One*, vol. 13, no. 8, pp. 1–17, 2018, doi: 10.1371/journal.pone.0201710.

[83] W. C. B. Joseph F. Hair Jr. and R. E. A. Barry J. Babin, *Multivariate Data Analysis (7th ed.)*, 7th ed. Cengage, 2019.

[84] B. Tjahjadi, N. Soewarno, A. A. P. Sutarsa, and J. Jermias, "Effect of intellectual capital on organizational performance in the Indonesian SOEs and subsidiaries: roles of open innovation and organizational inertia," *J. Intellect. Cap.*, vol. 25, no. 2–3, pp. 423–447, 2024, doi: 10.1108/JIC-06-2023-0140.

[85] S. Mohr and R. Kühl, "Acceptance of artificial intelligence in German agriculture: an application of the technology acceptance model and the theory of planned behavior," *Precis. Agric.*, vol. 22, no. 6, pp. 1816–1844, 2021, doi: 10.1007/s11119-021-09814-x.

[86] T. Teo, C. B. Lee, C. S. Chai, and S. L. Wong, "Assessing the intention to use technology among pre-service teachers in Singapore and Malaysia: A multigroup invariance analysis of the Technology Acceptance Model (TAM)," *Comput. Educ.*, vol. 53, no. 3, pp. 1000–1009, 2009, doi: 10.1016/j.compedu.2009.05.017.

[87] N. Thompson, T. J. McGill, and X. Wang, "'Security begins at home': Determinants of home computer and mobile device security behavior," *Comput. Secur.*, vol. 70, pp. 376–391, 2017, doi: 10.1016/j.cose.2017.07.003.

[88] D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," *Comput. Secur.*, vol. 48, pp. 281–297, 2015, doi: 10.1016/j.cose.2014.11.002.

[89] U. Kiran, N. F. Khan, H. Murtaza, A. Farooq, and H. Pirkkalainen, "Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory," *Comput. Secur.*, vol. 149, no. July 2024, p. 104204, 2024, doi: 10.1016/j.cose.2024.104204.

[90] R. Mousavi, R. Chen, D. J. Kim, and K. Chen, "Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory," *Decis. Support Syst.*, vol. 135, no. May, p. 113323, 2020, doi: 10.1016/j.dss.2020.113323.

[91] M. S. Joseph F. Hair Jr., William C. Black, Christian M. Ringle, G. Tomas M. hult, "A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)," *SAGE Publ.*, vol. 46, no. 1–2, pp. 184–185, 2022, doi: 10.1016/j.lrp.2013.01.002.

[92] B. Al-Ateeq, N. Sawan, K. Al-Hajaya, M. Altarawneh, and A. Al-Makhadmeh, "Big Data Analytics in Auditing and the Consequences for Audit Quality: a Study Using the Technology Acceptance Model (Tam)," *Corp. Gov. Organ. Behav. Rev.*, vol. 6, no. 1, pp. 64–78, 2022, doi: 10.22495/cgobrv6i1p5.

[93] A. F. Hayek, N. A. Noordin, and K. Hussainey, "Machine learning and external auditor perception: An analysis for UAE external auditors using technology acceptance model," *J. Account. Manag. Inf. Syst.*, vol. 21, no. 4, pp. 475–500, 2022, doi: 10.24818/jamis.2022.04001.

[94] D. Fischer-Preßler, D. Bonaretti, and K. Fischbach, "A Protection-Motivation Perspective to Explain Intention to Use and Continue to Use Mobile Warning Systems," *Bus. Inf. Syst. Eng.*, vol. 64, no. 2, pp. 167–182, 2022, doi: 10.1007/s12599-021-00704-0.

[95] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Inf.*, vol. 13, no. 9, 2022, doi: 10.3390/info13090413.

[96] E. J. Williams and A. N. Joinson, "Developing a measure of information seeking about phishing," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–16, 2020, doi: 10.1093/cybsec/tyaa001.

[97] F. L. Sylvester, "Mobile Device Users' Susceptibility to Phishing Attacks," *Int. J. Comput. Sci. Inf. Technol.*, vol. 14, no. 1, pp. 1–18, 2022, doi: 10.5121/ijcsit.2022.14101.

[98] K. J.S, K. G. P. Senani, and R. Ajward, "Examining determinants of auditors' intention to use CAATs in external auditing using an

extended UTAUT model; evidence from Sri Lanka," *J. Financ. Report. Account.*, no. July, 2024, doi: 10.1108/JFRA-08-2023-0474.

[99] A. U. Ardelia, C. F. Fangasadha, and R. Widuri, "Integrating Tam, Tpb, and Sct in Predicting Caats Adoption: a Triple Lens Approach," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 5, pp. 1615–1629, 2025.

[100] T. McGill and N. Thompson, "Exploring potential gender differences in information security and privacy," *Inf. Comput. Secur.*, vol. 29, no. 5, pp. 850–865, 2021, doi: 10.1108/ICS-07-2020-0125.