Journal of Theoretical and Applied Information Technology
28th February 2025. Vol.103. No.4

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

TOWARD SECURE AUDITING: A STUDY ON AUDITOR READINESS IN CYBERSECURITY IMPLEMENTATION USING EXTENDED UTAUT FRAMEWORKS

[1]NICHOLAS ZEFANYA ISKANDAR, [2]WILLIAM, [3]KEVIN DENISWARA
[1,2,3]Accounting Department, School of Accounting, Bina Nusantara University, Jakarta, 11480. Indonesia
Email: [1]nicholas.iskandar@binus.ac.id, [2]william088@binus.ac.id, [3]kdeniswara@binus.edu

ABSTRACT

This study explores cybersecurity's crucial role and integration within the audit process in enhancing information and data security in facing rising cyberattacks and data threats using the Extended Unified Theory of Acceptance and Use of Technology (UTAUT). Despite the critical nature of this integration, research models exploring the relationship between cybersecurity and auditing remain insufficiently studied. To address this gap, the research adopts a quantitative method to approach external auditors in public accounting firms in the Greater Jakarta area. Apart from the UTAUT framework, this study has adopted negative inhibitors from the Technological Readiness (TR) model to assess auditor perception on using new technology. The data were collected through questionaries and analyzed using SmartPLS. The findings show that auditors' behavioral intention to use cybersecurity is strongly influenced by performance expectancy, effort expectancy, facilitating conditions, and insecurity, where social influence and discomfort have no significant influence. By developing an extended UTAUT framework, this research aims to explore the readiness of external auditors to adopt cybersecurity within their audit process to improve audit performance and data security.
Keywords: *Cybersecurity, Audit, UTAUT, Technological Readiness (TR), Data Protection*

1. INTRODUCTION

The surge in technological advancements has significantly transformed the business landscape, encouraging organizations to adopt technological tools, and accelerating the digitization of all operational activities [1]. Razzaq et al., (2020) state that top management plays a critical driver in business strategy transformation, with 70% of top management prioritizes the adoption of technology to accelerate the company's performance. Furthermore, according to Canaday (2020), 63% of top management have allocated funds to digitally transforming their company. However, Jadhav, (2023) explains that the rise of digital transformation also comes with a surge in cyber risk and threats that can disrupt companies' operations and revenue.

In a survey conducted on 1,000 CEO by Accenture (2023), 74% of CEOs expressed concerns about their organization's ability to sustain and defend against cyberattacks. As time goes by, the level of losses due to cyber-attacks continues to increase. Cyber-attacks have been stated to be a prime threat and have increased by 300% since COVID-19 pandemic [3]. IBM Security and Ponemon Institute (2020) also revealed that the rapid number of cyberattacks is unsurprising, given that the average cost of a security breach has risen from $3.5m in 2006 to $9.4m in 2022. These incidents emphasize the importance of cybersecurity that become a new risk management dimension for a company [4]. Cybersecurity has become a top priority that is best handled by integrating it into managerial control system, which makes cybersecurity not just as a technical challenge, but also as an auditing matter especially for auditor [5]. According to its characteristics and best practices, cybersecurity has become a necessity that companies must have especially in the auditing processes [6].

In the report *risk in focus* by ECIIA, (2023) Cybersecurity and data security have been identified as the top threats faced by auditors in the next 3 years, which is supported in the ACFE report, (2022) showing that 25% involves forging electronic documents. Previous studies [7] also explained that data protection is changing the auditing landscape, emphasizing that everyone in the company need to be aware of the new risks involved in using data information. Therefore, it is important for auditors to be prepared to use cyber security technology as a data security solution while [8] also mentioned that support from organizations in developing cyber security skills is also important and very necessary to prepare auditors to mitigate cyber-attacks. These

emphasize that advances in technology mean that auditors are not only responsible for performing reasonable assurance about company financial statements, but auditors must also be able to identify, prevent, be aware of and deal with system vulnerabilities that have the potential to cause data theft.

This study is based of Unified Theory of Acceptance and Use of Technology (UTAUT) [9] and Technology Readiness (TR) [10] obtained in real-time using a questionnaire. The UTAUT Framework was chosen because it combines eight models that previously studied the usage behavior of technology. Moreover, we expand the UTAUT model with discomfort and insecurity to assess inhibiting factors in individual perceptions of using new technology. This study was conducted to examine Indonesian external auditor's readiness in integrating cybersecurity and data protection practices in their audits. Our paper focuses on the auditor's position in facing the increasing cyberattacks and data protection threats. In doing so, our paper provides an analysis in the extension of the auditor's role, enhances knowledge on damages suffered by organizations due to cyberattacks, and change in auditing practice in the era of technology with a focus on cybersecurity integration and data protection [7].

2. LITERATURE REVIEW

2.1 Cybersecurity in Auditing

Cybersecurity refers to the protection of systems, networks and data from various types of cyber threats. In the audit context, cyber security technology can be classified into four types, including as a tool for collecting information, assessing data vulnerabilities, penetration testing and forensic investment [11]. In a broader way, cyber security technology includes a variety of tools and techniques designed to protect data, systems and digital networks from various types of cyber threats. Previous research [12] states that topics related to cybersecurity audit are still a new dimension on security practices that aimed at supporting the protection of crucial company information. According to the Information Systems Audit and Control Association (ISACA), the COBIT framework can help in implementing best practices to improve an organization's IT governance system in the context of implementing cyber security technology. In this research, cybersecurity technology becomes a tool in monitoring network and IT system activities during the audit process. In [13], states that cyber security should be part of the structure of any organization or business. Additionally, in the research [14] states that cyber security technology has an important role in ensuring the confidentiality and integrity of data because it includes the implementation of strong access controls, encryption mechanisms and data validation techniques.

The contribution domain of cybersecurity technology leads to basic protection of data and information confidentiality, endpoint and cloud security, and mobile network security [15]. In [16] states that cyber security can be achieved through a distributed security system which consists of three intelligent services including, authentication, automation and interoperability. These security systems can enhance the data security system in audit practices. Data authentication and encryption systems can help businesses and even auditors in limiting access to crucial information or data they have. Can be seen in Figure 1. Standard data encryption scheme

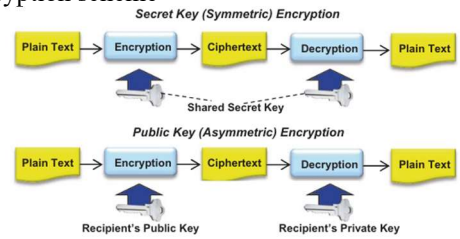

Figure 1. Basic Encryption Schemes [17]

As seen in Figure 1. Encryption data security is divided into two methods, namely with a secret key and a public key. In [17] explains that secret keys are given specifically to certain interested parties, while public keys eliminate this step. The process of collecting information during audit practices through various sources which is then centralized on one server or network can be one of the focuses in implementing security technology [11]. This is because all information that is held centrally requires a high security system so that it does not easily become a target for data theft, manipulation or other types of cyber-attacks. Therefore, in modern audit practices, auditors must have a deep understanding of various types of cybersecurity technologies.

2.2 Information System (IS) Success Model

Before the development of UTAUT model, the study of usage behavior is based on eight theoretical models, such as the *Technology Acceptance Model* (TAM), *Theory of Reasoned Action* (TRA), *Theory of Planned Behavior* (TPB), *Combined TAM and*

TPB (C-TAM-TPB), *Motivational Model* (MM), *Social Cognitive Theory* (SCT), *Innovation Diffusion Theory* (IDT) and *Model of PC Utilization* (MPCU). The Unified Theory of Adoption and Use of Technology (UTAUT), developed by [9], empirically reviews previous eight theoretical models regarding acceptance and use of a new technology. This model identifies four key variables that play an important role as determinants in user acceptance and usage behavior, consisting of performance expectancy, effort expectancy, social influence and facilitating conditions which are moderated by moderating variables such as gender, age, experience, and voluntariness of use [9].

Based on [18], individual perception is a necessary first step that needs to be considered toward identifying and qualifying the psychological processes of the perceptions of a technology's value. Therefore, we use technology readiness (TR) to measure the auditor's general technology belief towards using *Cybersecurity*. Technology Readiness (TR) is a comprehensive framework that assess individual behavior to accept and utilize new technology [10]. TR was developed with four dimensions that can be predictors of behavior related to technology use, consisting of optimism, innovativeness, discomfort and insecurity. These four dimensions are grouped into two categories compromise of motivating factors (optimism and innovativeness) and inhibiting factors (discomfort and insecurity) that work together to form the user's view of technology. High levels of discomfort and insecurity can hinder the adoption of technology, on the other hand, high levels of optimism will encourage the adoption of a new technology because they are aware of its potential benefits.

After comprehensively reviewing both theories of technology acceptance and readiness (UTAUT and TRI) and considering the problems currently occurring in this research. Therefore, this study directly uses factors from the Unified Theory of Adoption and Use of Technology (UTAUT) to understand the extent to which cyber security technology can be accepted by auditors and two selected factors from the Technology Readiness (TR) model, namely discomfort and insecurity, are examined as inhabiting factors for auditor readiness in accepting the use of cyber security technology in audit activities. UTAUT was chosen as a theoretical basis because it covers factors that comprehensively influence auditors' acceptance of the use of cyber security technology. Meanwhile, the discomfort and insecurity factor from TR was chosen as a support in looking at the hindrance felt by auditors in interacting with cyber security technology. Previous researchers have used some or all of the factors in UTAUT and TR and investigated the influence of these factors on: the adoption of computer-assisted audit techniques among internal auditors [19], [20], intentions users in adopting AI-based cyber security systems in the UAE [21], behavioral intentions of external auditors in using audit software [22], readiness of auditors in public accounting firms in using digital technology [23]. Several studies in the audit context have used the UTAUT framework and found the influence of performance expectations, effort expectations, and social influences on auditors in adopting new technology. However, an auditor's lack of control and distrust in the performance of cybersecurity technology can reduce the intention to adopt the technology.

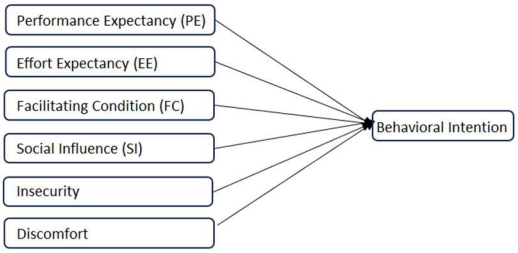

Figure 2. Conceptual Framework

2.3 Hypothesis Development

2.3.1 Performance Expectancy

Performance expectancy is defined as the degree to which an individual believes that the use of technology can help him or her to achieve improvement in job performance [9]. A study by [22] revealed that performance expectancy has a significant effect on behavioral intention. Similar results also shown in the research by [24] which found that performance expectancy does significantly affect behavioral intention on adoption of technology. In the context of auditing, we predict that when auditors gain benefits by using *cybersecurity*, auditors will more likely intend to use *cybersecurity* in the audit process, but if auditors do not get benefits from using cybersecurity, the level of willingness to use a cyber security system will decrease. Therefore, the following hypothesis was formulated:

H1: ***Performance Expectancy has a positive impact on Behavioral Intention to use cybersecurity***

2.3.2. Effort Expectancy

Effort Expectancy is the perception of the user on the amount of effort it will take to utilize the new technology [9]. Similar research related to technology adoption also stated that users are more likely to continue utilizing a new technology if their experience with the technology went smoothly and trouble-free [25]. Furthmore, it is found that the lower effort needed in adapting a new technology will result in a higher intent to accept it [26]. This result contradicts Siswanto et al (2018), which does not find effort expectancy to have a significant impact in the adoption of technology. Therefore, the following hypothesis was formulated:

H2: ***Effort Expectancy has a positive impact on Behavioral Intention to use cybersecurity***

2.3.3. Social Influence

Social Influence is the external pressure created within the user's environment in which technology has been adapted [9]. People when faced with uncertainty and lack of understanding with new technology tend to look for assurance and validation from their closest friends, in this case their work environment [27]. In the research Tseng et al., (2022) also shows similar result showing social influence does affected the user's behavioral intention. However, contradiction was found in the research by [22]. Thus, the following hypothesis was formulated:

H3: ***Social Influence has a positive impact on Behavioral Intention to use cybersecurity***

2.3.4. Facilitating Conditions

Facilitating Conditions refers to the user's surroundings' ability to provide the resources to support the adaptation of the new technology [9]. In existing research shows that users who are provided with such resources can adapt new technology smoothly [27]. The availability of facilitating conditions to utilize cybersecurity positively affects the behavioral intentions of the user [29]. However, this result contradicts Siswanto et al., (2018), which does not find facilitating conditions to have a significant impact and be a supporting factor in the adoption of technology. Thus, the following hypothesis was formulated:

H4: Facilitating Conditions has a positive impact on Behavioral Intention to use cybersecurity

2.3.5. Insecurity

Insecurity acts as a negative emotion and inhibitor in the Technology Readiness model. Insecurity affects the user's perception and emotion towards adaptation of new technology [10]. Similar research related to technology adoption has also explained that a high insecurity indicates that the user is more likely to be skeptical and distrust the capability and performance of the new technology [31]. In the application of cybersecurity, user who experienced higher insecurity may associate adaptation of new technology with risks. Lack of confidence in the technology negatively affects the Behavioral Intention [32]. Thus, the following hypothesis was formulated:

H5: ***Insecurity has a negative impact on Behavioral Intention to use cybersecurity***

2.3.6. Discomfort

Discomfort is associated with the user's believe that they have little to no control over technology and may be overwhelmed with the adaptation of new technology [10]. Discomfort acts as a negative emotion and inhibitor in the TR model. In the research by Humbani & Wiese, (2018), it is found that a high level of discomfort of technology leads to unfavorable intention to use the technology. In the auditing context, auditors who have a high level of discomfort will feel overwhelmed by the technology that eventually decrease the behavioral intention to use the systems. Therefore, the following hypothesis was formulated:

H6: ***Discomfort has a negative impact on Behavioral Intention to use cybersecurity***

3. RESEARCH METHODOLOGY

The research studies auditors in Public Accounting Firms as the main subject and was done using quantitative methods, specifically with a questionnaire using Google Forms as the main platform. All the items were adapted and then adjusted from Venkatesh (2003) for Unified Theory of Acceptance and Use of Technology (UTAUT) and Parasuraman (2000) for Technology Readiness. The questionnaire consists of 44 questions divided into 3 sections: one section focused on gathering information about the respondents (name, age, job

position, experience, and firm's category), while the remaining sections explored theoretical concepts to assess auditors' responses. To avoid respondents being "neutral", the questionnaire was designed using a four-point Likert Scale for all items, ranging from 1 (strongly disagree) to 4 (strongly agree) [34]. In conducting data analysis, this research performed PLS-SEM (Partial Least Squares Structural Equation Modeling) processed using SmartPLS version 4. The questionnaire obtained 143 sample of auditors with a minimum position of junior auditor at public accounting firms located in the Greater Jakarta are. The characteristics of the sample can be found in Table 1.

Table 1 Descriptive Statistics

Characteristics of Respondents		Total	Percentage
Gender	Male	81	56.64%
	Female	62	43.36%
Age (years)	20 - 30 years old	92	64.34%
	31 - 40 years old	48	33.57%
	41 - 50 years old	3	2.10%
Position	Junior Auditor	83	58.04%
	Senior Auditor	56	39.16%
	Assistant Manager	2	1.40%
	Manager	2	1.40%
Experience	1 - 5 years	94	65.73%
	6 - 10 years	46	32.17%
	11 - 15 years	3	2.10%
KAP	Big 4	130	90.91%
Category	Non Big 4	13	9.09%

4. RESULT

4.1 Validity Test

A convergent validity test is applied to test the validity, accuracy, and competency of the data used in this research before being proceed in the next testing model. The convergent validity examines the readability of data, research indicators, and correlation between variables within the research model [35]. The table of validity test result is shown below

Table 2 Validity Test

Construct	Code	Outer Loading	AVE	Results
Performance Expectancy	PE1	0.878	0.717	Valid
	PE2	0.822		Valid
	PE3	0.847		Valid
	PE4	0.838		Valid
Effort Expectancy	EE1	0.854	0.743	Valid
	EE2	0.857		Valid
	EE3	0.852		Valid
	EE4	0.885		Valid
Social Influence	SI1	0.872	0.757	Valid
	SI2	0.879		Valid
	SI3	0.865		Valid
	SI4	0.864		Valid
Facilitating Condition	FC1	0.782	0.653	Valid
	FC2	0.851		Valid
	FC3	0.789		Valid
	FC4	0.808		Valid
Insecurity	INS1	0.784	0.652	Valid
	INS2	0.795		Valid
	INS3	0.811		Valid
	INS4	0.757		Valid
	INS5	0.863		Valid
	INS6	0.799		Valid
	INS7	0.835		Valid
	INS8	0.814		Valid
	INS9	0.803		Valid
Discomfort	DC1	0.842	0.740	Valid
	DC2	0.846		Valid
	DC3	0.861		Valid
	DC4	0.859		Valid
	DC5	0.871		Valid
	DC7	0.876		Valid
	DC8	0.869		Valid
	DC9	0.874		Valid
	DC10	0.846		Valid
Behavioral Intention	BI1	0.856	0.707	Valid
	BI2	0.823		Valid
	BI3	0.838		Valid
	BI4	0.845		Valid

In Structural Equation Modeling (SEM) and Confirmatory Factor Analysis (CFA), a construct's validity can be tested using loading factors and Average Variance Extracted (AVE). An indicator is deemed valid on the convergent validity test if their outer loading results is greater than 0.70 and greater than the AVE of at least 0.5, indicators that does not pass the test will be eliminated from the research model. The results show that the construct meets the AVE threshold, Behavioral Intention has an AVE at 0.707, Discomfort at 0.740, Effort Expectancy at 0.743, Facilitating Condition at 0.653, Insecurity at 0.652, Performance Expectancy at 0.717, and Social Influence at 0.757, indicating a valid construct. However, indicator DC6 does not pass the outer loading threshold with 0.586. Therefore, indicator DC6 will be removed from the research model [36].

4.2 Hypothesis Testing

The study utilized PLS-SEM to evaluate the hypothesis through a methodical approach. Most of the questions were confirmed valid, as factor loadings surpassed the 0.5 & 0.7 threshold, with one indicator being eliminated because it did not exceed the threshold limit. After confirming validity, the reliability test must be carried out to ensure that the data used is dependable, thereby enhancing the overall value of the study [37]. The reliability was assessed by examining Cronbach's alpha and Composite Reliability (CR). Cronbach's alpha measures the internal consistency of individual items, while composite reliability evaluates the dataset's overall reliability. For the data to be

considered reliable, both values must reach at least 0.6.

Table 3 Reliability Test

Construct	Code	Outer Loading	Cronbach's Alpha	CR
Performance Expectancy	PE1	0.878	0.868	0.910
	PE2	0.822		
	PE3	0.847		
	PE4	0.838		
Effort Expectancy	EE1	0.854	0.885	0.921
	EE2	0.857		
	EE3	0.852		
	EE4	0.885		
Social Influence	SI1	0.872	0.893	0.926
	SI2	0.879		
	SI3	0.865		
	SI4	0.864		
Facilitating Condition	FC1	0.782	0.823	0.883
	FC2	0.851		
	FC3	0.789		
	FC4	0.808		
Insecurity	INS1	0.784	0.934	0.944
	INS2	0.795		
	INS3	0.811		
	INS4	0.757		
	INS5	0.863		
	INS6	0.799		
	INS7	0.835		
	INS8	0.814		
	INS9	0.803		
Discomfort	DC1	0.842	0.956	0.962
	DC2	0.846		
	DC3	0.861		
	DC4	0.859		
	DC5	0.871		
	DC7	0.876		
	DC8	0.869		
	DC9	0.874		
	DC10	0.846		
Behavioral Intention	BI1	0.856	0.862	0.906
	BI2	0.823		
	BI3	0.838		
	BI4	0.845		

Based on the result, it reveals that all constructs meet the required reliability threshold. The Performance Expectancy construct exhibited strong reliability, with Cronbach's alpha 0.868 & composite reliability 0.910. The Effort Expectancy construct showed similar strength, with both Cronbach's alpha (0.885) and composite reliability (0.921). The social influence construct accessibility demonstrated particularly strong reliability, with a Cronbach's alpha of 0.893 and composite reliability of 0.926. The Facilitating Condition construct also performed well, with a Cronbach's alpha of 0.823 and composite reliability of 0.883. Lastly, both the discomfort and insecurity construct also met the reliability criteria with Cronbach's alpha value of 0.956 and 0.934, respectively, and composite reliability value of 0.962 and 0.944.

Following the reliability and reliability test, all qualified data are analyzed to evaluate the research hypothesis. Hypothesis testing performed using the two-tailed approach with a 95% confidence level. According to Cleff, (2019) a 0.05 p-value & t-value greater than 1.96 is required for the hypothesis to be accepted. The bootstrapping approach was used to calculate and determine whether the hypothesis meet the required threshold. The result of hypothesis testing for each theoretical construct are shown in table below:

Table 4 Hypothesis Testing (Bootstrapping)

Construct	T-Statistic	P-Values
PE --> BI	2.701	0.007
EE --> BI	3.440	0.001
SI --> BI	1.620	0.105
FC --> BI	2.604	0.009
INS --> BI	2.145	0.032
DC --> BI	0.677	0.498

The hypothesis testing of effort expectancy on behavioral intention to use cybersecurity shows a T-statistical value of 3.440 with P-value of 0.001. This computation indicates that an auditor's effort expectancy has an impact in their intention to adopt cybersecurity into their work process. The hypothesis is accepted as it meets the required T-value and P-value (Jogiyanto & Abdillah, 2016)

The computation of facilitating condition towards behavioral intention shows a result of T-statistical value of 2.604 and P-value of 0.009, the result suggests that the presence of supporting facilities and resources such as technologies would give an impact on the auditor's behavioral intention to use cybersecurity, resulting in the acceptance of the hypothesis as it has met the required threshold. Insecurity's hypothesis is supported as the computation result on auditor's insecurity towards their behavioral intention to use auditor shows a result of T-statistical value 2.145 and P-value of 0.032. This suggests that auditor's insecurity has an impact towards the adoption of cybersecurity. Thus, the hypothesis can be accepted.

Performance Expectancy is found to have an impact on auditor's behavioral intention in using cybersecurity. The computation shows a result of T-statistical value 2.701 and P-value of 0.007, as the results pass the threshold, this would suggest that auditor's expectation towards how cybersecurity could help improve their work performance will

impact their intention to use cybersecurity. Hence, the hypothesis can be supported.

According to the result, the influence of discomfort on behavioral intention to use cybersecurity has a T-statistical value of 0.677 with P-value of 0.498. This computation indicates that an auditor's discomfort attitude towards cybersecurity has no impact on their intention to use the cybersecurity system. Thus, the hypothesis was rejected since it does not meet the required T-value and P-value [38].

Lastly, the effect of social influence on behavioral intention to use cybersecurity also does not meet the required value. The computation result showed a T-statistical value of 1.620 and P-value of 0.105, indicating that a social influence of an auditor has no impact on behavioral intention to use cybersecurity system. Thus, the hypothesis was rejected.

5. DISCUSSION

Hypothesis 1 explore how performance expectancy relates to auditor's behavioral intention to use cybersecurity in their work process. The research reveals that auditors' willingness in utilizing the cybersecurity system is positively correlate with their perceived benefit. This is consistent with previous research conducted by Bierstaker et al., (2014) stated that performance expectancy significantly affects the usage of technology by auditors working in firms due to the high expectation of performance output. Similarly, Abdul Ghani et al., (2022) stated that the usage of technology in the audit process can influence the audit quality, this indicates that the adoption of a system such as cybersecurity could influence how auditors perform based on how beneficial technology is towards their performance. Previous research done indicates that auditors as a profession is highly motivated by performance expectancy put on by audit firms, thus technology such as cybersecurity that benefits auditor's performance results in a significant impact in the relation of performance expectancy towards a higher behavioral intention to use technology.

In hypothesis 2, the connection of effort expectancy towards auditor's behavioral intention to use cybersecurity in their work process is studied. The research result reveals a strong correlation between how complexity affect auditors' willingness to utilize technology, an easier utilization will increase their willingness to utilize the cybersecurity system. This result is aligned with previous studies done [22], [40]. Tansil et al., (2019) states in their research that in adopting a new system, auditors prefer to use an easy-to-use system that requires lower effort and less time consuming compared to a more complex system. [40] found that auditors in Egypt have a higher tendency to accept the adoption of a new system to their work process if the system does not require intensive effort and possesses basic features, in line with the research result conducted towards Indonesian auditors. The result in this research suggests that audit firms can choose to adopt a cybersecurity system that takes less effort and possesses basic features to increase auditor's behavioral intention to use the cybersecurity system.

Hypothesis 3 addresses the connection between social influence and auditor's intention to use cybersecurity. The finding show that social influence does not have an impact on behavioral intention, indicating that external social pressure do not play a role in their adoption of cybersecurity systems. These findings are in line with previous research by [19], [22]. Tansil et al., (2019), who state that auditors' decisions to use a systems are driven by their personal expertise and beliefs, rather than social factors. Abdul Ghani et al., (2022) also stated that the decisions to adapt new technologies are primarily influenced by personal considerations such as perceived usefulness and ease of use, with social influence appears to have a minimal role in their decision-making process. This indicates that auditors' decisions to use cybersecurity are more rational and logical, which relies more on personal assessments of the cybersecurity benefits and risks. The behavioral intention to use cybersecurity will be further influenced by key factors such as the perceived ability of cybersecurity systems to mitigate risks and the availability of adequate training and support.

Hypothesis 4 studies the association between facilitating condition and auditor's behavioral intention to use cybersecurity in their work process. Evidence from the research indicates that facilitating conditions has a significant impact on behavioral intention, it is highlighted that auditors who are supported by firm through facilities are more likely intend to use cybersecurity in their work process. The results are supported by research conducted by Mansour, (2016) who states that there's a positive correlation between facilitating conditions and auditors' intention to use technology. Similar research conducted by Ali et al., (2022) also argued that facilitating condition such as receiving training

can increase someone's intention to use the systems. This suggests that a supportive firm that provides essential resources, training, and technical support plays a significant role to increase auditor's behavioral intention to use the cybersecurity system.

Hypothesis 5 proposes the analysis of insecurity's relation towards auditor's behavioral intention to use cybersecurity in their work process. The research underscores the significant negative impact that insecurity have on behavioral intention, indicating that when auditors' feel insecure about their ability in using cybersecurity, they are less likely to use cybersecurity in their work process. The result align with the research done by [31] who stated that when individuals feel distrust and lack of confidence over a technology, they will more likely to be sceptical and typically has a low intention to adopt the technology. When it comes to Cybersecurity, auditors often feel a lack of confidence about the capability of cybersecurity due to its complexion which then hinders their willingness to use the cybersecurity system.

Hypothesis 6 investigates whether discomfort influences auditors' behavioral intention to adapt cybersecurity. The research result implies that auditors' uneasiness in using a cybersecurity system does not significantly influence their intent to use the system. Negm, (2023) supports this result, indicating discomfort does not affect technology adoption, as users' intention is primarily driven by the technology's usefulness. Humbani & Wiese, (2018) also stated that discomfort does not affect auditor's intention to use technology provided that the technology to adopt provides beneficial outcome, is intuitive, and commonly used within the work process.

The overall result from the hypothesis testing indicates that when implementing cybersecurity, audit firms should focus on facilitating technologies in supporting the implementation of the cybersecurity technology, it is important to have features in enhancing auditors' performance while also ensuring an easy-to-use system to ensure that auditors are confident in operating the system.

6. CONCLUSION

The rise of technology has increased the occurrence of cyber risk and threats, the adoption of cybersecurity has become a necessity for companies and firms to ensure data protection and mitigation of cyberattacks. This research aims to study the auditor's readiness in cybersecurity implementation using the UTAUT and TR framework. The research is supported by the development of 6 hypothesis and confirms that 4 have a positive impact and 2 negative impacts. The result confirms performance expectancy (PE), effort expectancy (EE), facilitating condition (FC), and insecurity (INS) affecting auditor's behavioral intention (BI) to use cybersecurity, conversely social influence (SI) and discomfort (DC) does not affect the behavioral intention (BI). In addition, the result could encourage top management and auditors in the implementation of cybersecurity facing the prominent problem of cyberthreats and evolving role of auditors [43].

The limitation of this research is that the data composition of respondents such as age, gender, experience, and KAP category may directly or indirectly influence on the behavioral intention to use. In addition, the lack of previous research and studies on cybersecurity relationship with auditors have presented a significant challenge and limited perspective. Further research should explore moderating factors such as auditor's experience in utilizing auditing tools and software in their work process, along with how cybersecurity measures play a role within internal audit profession '

REFERENCES

[1] K. Jadhav, "the Role of Cyber Security Audits," no. April, pp. 0–7, 2023.
[2] A. Razzaq, S. Azirah Asmal, M. Saad Talib, N. Ibrahim, and A. Mohammed, "Cloud ERP in Malaysia: Benefits, Challenges, and Opportunities," *Int. J. Adv. Trends Comput. Sci. Eng.*, 2020, doi: 10.30534/ijatcse/2020/85952020.
[3] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technology Letters*. 2021. doi: 10.1002/itl2.247.
[4] E. Haapamäki and J. Sihvonen, "Cybersecurity in accounting research," *Managerial Auditing Journal*. 2019. doi: 10.1108/MAJ-09-2018-2004.
[5] L. A. Gordon, M. P. Loeb, T. Sohail, C. Y. Tseng, and L. Zhou, "Cybersecurity, capital allocations and management control systems," *Eur. Account. Rev.*, 2008, doi: 10.1080/09638180701819972.
[6] S. Slapničar, T. Vuko, M. Čular, and M. Drašček, "Effectiveness of cybersecurity audit," *Int. J. Account. Inf. Syst.*, 2022, doi: 10.1016/j.accinf.2021.100548.
[7] M. La Torre, V. L. Botes, J. Dumay, and E.

Odendaal, "Protecting a new Achilles heel: the role of auditors within the practice of data protection," *Manag. Audit. J.*, 2019, doi: 10.1108/MAJ-03-2018-1836.

[8] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," *J. Inf. Secur. Appl.*, 2021, doi: 10.1016/j.jisa.2020.102726.

[9] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Q. Manag. Inf. Syst.*, 2003, doi: 10.2307/30036540.

[10] A. Parasuraman, "Technology Readiness Index (Tri): A Multiple-Item Scale to Measure Readiness to Embrace New Technologies," *J. Serv. Res.*, 2000, doi: 10.1177/109467050024001.

[11] O. M. M. Al-Matari, I. M. A. Helal, S. A. Mazen, and S. Elhennawy, "Integrated framework for cybersecurity auditing," *Inf. Secur. J.*, 2021, doi: 10.1080/19393555.2020.1834649.

[12] M. S. Islam, N. Farah, and T. F. Stafford, "Factors associated with security/cybersecurity audit by internal audit function: An international study," *Manag. Audit. J.*, 2018, doi: 10.1108/MAJ-07-2017-1595.

[13] S. Wertheim, "Auditing for Cybersecurity Risk.," *CPA J.*, 2019.

[14] S. Bozkus Kahyaoglu and K. Caliyurt, "Cyber security assurance process from the internal audit perspective," *Manag. Audit. J.*, 2018, doi: 10.1108/MAJ-02-2018-1804.

[15] B. F. Martins, L. Serrano, J. F. Reyes, J. I. Panach, O. Pastor, and B. Rochwerger, "Conceptual Characterization of Cybersecurity Ontologies," in *Lecture Notes in Business Information Processing*, 2020. doi: 10.1007/978-3-030-63479-7_22.

[16] H. Katzan, Jr., "Cybersecurity Service Model," *J. Serv. Sci.*, 2012, doi: 10.19030/jss.v5i2.7576.

[17] J. M. Borky and T. H. Bradley, "Protecting Information with Cybersecurity," in *Effective Model-Based Systems Engineering*, 2019. doi: 10.1007/978-3-319-95669-5_10.

[18] C. H. Lin, H. Y. Shih, and P. J. Sher, "Integrating technology readiness into technology acceptance: The TRAM model," *Psychol. Mark.*, 2007, doi: 10.1002/mar.20177.

[19] A. Abdul Ghani, S. Shahimi, and A. A. Che Azmi, "DETERMINANTS OF COMPUTER ASSISTED AUDIT TOOLS AND TECHNIQUES (CAATs) ADOPTION," *Adv. Int. J. Banking, Account. Financ.*, 2022, doi: 10.35631/aijbaf.412001.

[20] A. Almagrashi, A. Mujalli, T. Khan, and O. Attia, "Factors determining internal auditors' behavioral intention to use computer-assisted auditing techniques: an extension of the UTAUT model and an empirical study," *Futur. Bus. J.*, 2023, doi: 10.1186/s43093-023-00231-2.

[21] 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.*, 2023, doi: 10.28945/5166.

[22] A. Y. M. Tansil, R. Widuri, A. Gui, and M. M. Ali, "Generalised Audit Software use by external auditor: An empirical examination from UTAUT," *Int. J. Innov. Creat. Chang.*, 2019.

[23] H. Susanto, A. J. Pramono, B. Akbar, and S. Suwarno, "The Adoption and Readiness of Digital Technologies Among Auditors in Public Accounting Firms: A Structural Equation Modeling Analysis," *Res. Horiz.*, 2023.

[24] C. Buabeng-Andoh and C. Baah, "Pre-service teachers' intention to use learning management system: an integration of UTAUT and TAM," *Interact. Technol. Smart Educ.*, 2020, doi: 10.1108/ITSE-02-2020-0028.

[25] A. Gunasinghe, J. A. Hamid, A. Khatibi, and S. M. F. Azam, "The adequacy of UTAUT-3 in interpreting academician's adoption to e-Learning in higher education environments," *Interact. Technol. Smart Educ.*, 2020, doi: 10.1108/ITSE-05-2019-0020.

[26] K. K. Soong, E. M. Ahmed, and K. S. Tan, "Factors influencing Malaysian small and medium enterprises adoption of electronic government procurement," *J. Public Procure.*, 2020, doi: 10.1108/JOPP-09-2019-0066.

[27] M. B. Ali, R. Tuhin, M. A. Alim, M. Rokonuzzaman, S. M. Rahman, and M. Nuruzzaman, "Acceptance and use of ICT in tourism: the modified UTAUT model," *J. Tour. Futur.*, 2022, doi: 10.1108/JTF-06-2021-0137.

[28] T. H. Tseng, S. Lin, Y. S. Wang, and H. X. Liu, "Investigating teachers' adoption of MOOCs: the perspective of UTAUT2," *Interact. Learn. Environ.*, 2022, doi: 10.1080/10494820.2019.1674888.

[29] S. Rahi, M. M. Othman Mansour, M. Alghizzawi, and F. M. Alnaser, "Integration of UTAUT model in internet banking adoption context," *J. Res. Interact. Mark.*, 2019, doi: 10.1108/jrim-02-2018-0032.

[30] T. Siswanto, R. Shofiati, and H. Hartini, "Acceptance and Utilization of Technology (UTAUT) as a Method of Technology Acceptance Model of Mitigation Disaster Website," in *IOP Conference Series: Earth and Environmental Science*, 2018. doi: 10.1088/1755-1315/106/1/012011.

[31] R. K. Kampa, "Combining technology readiness and acceptance model for investigating the acceptance of m-learning in higher education in India," *Asian Assoc. Open Univ. J.*, 2023, doi: 10.1108/AAOUJ-10-2022-0149.

[32] M. F. Chen and N. P. Lin, "Incorporation of health consciousness into the technology readiness and acceptance model to predict app download and usage intentions," *Internet Res.*, 2018, doi: 10.1108/IntR-03-2017-0099.

[33] M. Humbani and M. Wiese, "A Cashless Society for All: Determining Consumers' Readiness to Adopt Mobile Payment Services," *J. African Bus.*, 2018, doi: 10.1080/15228916.2017.1396792.

[34] D. Beglar and T. Nemoto, "Developing Likert-scale questionnaires," *JALT2013 Conf. Proc.*, 2014.

[35] F. Hair, Joe, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM", European Business Review," *Eur. Bus. Rev.*, 2018.

[36] T. Cleff, *Applied Statistics and Multivariate Data Analysis for Business and Economics: A Modern Approach Using SPSS, Stata, and Excel*. 2019. doi: 10.1007/978-3-030-17767-6.

[37] J. W. Creswell, "Research Design: Qualitative, Quantitative and Mixed Method Aproaches (3rd ed.)," *SAGE Publ.*, 2007.

[38] I. Ghozali and H. Latan, *Konsep, Teknik Dan Aplikasi Menggunakan Program Smart PLS 3.0*. 2015.

[39] J. Bierstaker, D. Janvrin, and D. J. Lowe, "What factors influence auditors' use of computer-assisted audit techniques?," *Adv. Account.*, 2014, doi: 10.1016/j.adiac.2013.12.005.

[40] H. J. Kim, A. Kotb, and M. K. Eldaly, "The use of generalized audit software by Egyptian external auditors: The effect of audit software features," *J. Appl. Account. Res.*, 2016, doi: 10.1108/JAAR-10-2015-0079.

[41] E. M. Mansour, "Factors Affecting the Adoption of Computer Assisted Audit Techniques in Audit Process: Findings from Jordan," *Bus. Econ. Res.*, 2016, doi: 10.5296/ber.v6i1.8996.

[42] E. Negm, "Internet of Things (IoT) acceptance model – assessing consumers' behavior toward the adoption intention of IoT," *Arab Gulf J. Sci. Res.*, 2023, doi: 10.1108/AGJSR-09-2022-0183.

[43] I. Friday and I. Japhet, "Information technology and the accountant today: What has really changed?," *J. Account. Tax.*, 2020, doi: 10.5897/jat2019.0358.