Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute
InformingScience.org

IJIKM.org

Volume 18, 2023

FACTORS INFLUENCING USER'S INTENTION TO ADOPT AI-BASED CYBERSECURITY SYSTEMS IN THE UAE

Mohammed Rashed Mohamed Al Humaid Alneyadi
School of Management, Universiti Sains Malaysia, Malaysia
Mohammed.alneyadi@student.usm.my

Md Kassim Normalini *
School of Management, Universiti Sains Malaysia, Malaysia and Graduate School of Management, Management & Science University, Malaysia
normalini@usm.my

* Corresponding author

ABSTRACT

Aim/Purpose
The UAE and other Middle Eastern countries suffer from various cybersecurity vulnerabilities that are widespread and go undetected. Still, many UAE government organizations rely on human-centric approaches to combat the growing cybersecurity threats. These approaches are ineffective due to the rapid increase in the amount of data in cyberspace, hence necessitating the employment of intelligent technologies such as AI cybersecurity systems. In this regard, this study investigates factors influencing users' intention to adopt AI-based cybersecurity systems in the UAE.

Background
Even though UAE is ranked among the top countries in embracing emerging technologies such as digital identity, robotic process automation (RPA), intelligent automation, and blockchain technologies, among others, it has experienced sluggish adoption of AI cybersecurity systems. This selectiveness in adopting technology begs the question of what factors could make the UAE embrace or accept new technologies, including AI-based cybersecurity systems. One of the probable reasons for the slow adoption and use of AI in cybersecurity systems in UAE organizations is the employee's perception and attitudes towards such intelligent technologies.

Methodology
The study utilized a quantitative approach whereby web-based questionnaires were used to collect data from 370 participants working in UAE government

Accepting Editor Ahmad Samed Al-Adwan │ Received: April 20, 2023 │ Revised: June 13, June 19, 2023 │ Accepted: June 24, 2023.
Cite as: Alneyadi, M. R. M. A. H., & Normalini, M. K. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. *Interdisciplinary Journal of Information, Knowledge, and Management*, *18,* 459-486. https://doi.org/10.28945/5166

organizations considering or intending to adopt AI-based cybersecurity systems. The data was analyzed using the PLS-SEM approach.

Contribution

The study is based on the Protection Motivation Theory (PMT) framework, widely used in information security research. However, it extends this model by including two more variables, job insecurity and resistance to change, to enhance its predictive/exploratory power. Thus, this research improves PMT and contributes to the body of knowledge on technology acceptance, especially in intelligent cybersecurity technology.

Findings

This paper's findings provide the basis from which further studies can be conducted while at the same time offering critical insights into the measures that can boost the acceptability and use of cybersecurity systems in the UAE. All the hypotheses were accepted. The relationship between the six constructs (perceived vulnerability (PV), perceived severity (PS), perceived response efficacy (PRE), perceived self-efficacy (PSE), job insecurity (JI), and resistance to change (RC)) and the intention to adopt AI cybersecurity systems in the UAE was found to be statistically significant. This paper's findings provide the basis from which further studies can be conducted while at the same time offering critical insights into the measures that can boost the acceptability and use of cybersecurity systems in the UAE.

Recommendations for Practitioners

All practitioners must be able to take steps and strategies that focus on factors that have a significant impact on increasing usage intentions. PSE and PRE were found to be positively related to the intention to adopt AI-based cybersecurity systems, suggesting the need for practitioners to focus on them. The government can enact legislation that emphasizes the simplicity and awareness of the benefits of cybersecurity systems in organizations.

Recommendations for Researchers

Further research is needed to include other variables such as facilitating conditions, AI knowledge, social influence, and effort efficacy as well as other frameworks such as UTAUT, to better explain individuals' behavioral intentions to use cybersecurity systems in the UAE.

Impact on Society

This study can help all stakeholders understand what factors can increase users' interest in investing in the applications that are embedded with security. As a result, they have an impact on economic recovery following the COVID-19 pandemic.

Future Research

Future research is expected to investigate additional factors that can influence individuals' behavioral intention to use cybersecurity systems such as facilitating conditions, AI knowledge, social influence, effort efficacy, as well other variables from UTAUT. International research across nations is also required to build a larger sample size to examine the behavior of users.

Keywords

AI, cybersecurity systems, UAE, protection motivation theory (PMT), intelligent systems, cyber threats, information security

INTRODUCTION

Artificial intelligence (AI) has become one of the core technologies with great potential to enhance cybersecurity in organizations. AI pertains to developing and using intelligent machines, which simulate intelligent human behavior, such as thinking, learning, reasoning, and planning, to solve complex problems (Dilek et al., 2015). Over the years, cybersecurity attacks have grown significantly and become more complex, rendering traditional human-centric strategies less effective (Ramírez, 2017; Salloum et al., 2020). This is despite the significant investments organizations have made in cybersecurity. Estimates in 2017 showed that major organizations globally spent, on average, US $3.8-16.8 million on cybersecurity (losses, recruitment of cybersecurity professionals, and implementation of cybersecurity measures) (Taddeo, 2019). In the UAE, various measures have been taken to improve cybersecurity, including the establishment of the Signals Intelligence Agency (SIA) whose primary role is to develop compliance standards to protect information and communications infrastructure. These standards are mandatory for government agencies and other critical sectors in the country and include prevention, detection, response, recovery, collaboration, and building cybersecurity capacity.

A 2019 study by the DarkMatter Group showed that the UAE accounts for about 5% of the world's cyber-attacks, which have increased by 55% in the past five years (DarkMatter Group, 2019). The UAE and other countries in the Middle East suffer from various cybersecurity vulnerabilities that are widespread and go undetected (DarkMatter Group, 2019; Guven, 2018). The UAE is also among the top targets of malware-class attacks and other techniques of cybercrimes such as credit/debit cards and denial-of-service (DoS) attacks (Chandra et al., 2019). According to the UAE's Telecommunication Regulations Authority (UTRA), UAE experienced more than 86 new cyber-attacks in 2018, among them Careem data violations, which enabled access of more than 14 million personal accounts to unauthorized users (Chandra et al., 2019).

Coincidentally, UAE is integrating technologies such as cyber-physical systems (CPS) and the internet of things (IoT). With such technological developments, robust cybersecurity approaches are needed since the advancement and expansion of digital infrastructure will undoubtedly create more space for cybercriminals to exploit. Worryingly, many UAE organizations have not considered cybersecurity as a significant aspect of digital infrastructural development as they still rely on human-centric approaches to combat cybersecurity threats (Al-Khater et al., 2020; Guven, 2018). The success of such systems, as mentioned earlier, is limited because of the rapid increase in the amount of data to be analyzed. This shows a need to employ intelligent technologies that can effectively handle the voluminous, complex data in cyberspace.

Even though UAE is ranked among the top countries in embracing emerging technologies such as digital identity, robotic process automation (RPA), intelligent automation, and blockchain technologies, among others, it has experienced sluggish adoption of AI cybersecurity systems (Editor's Desk, 2020; Malek, 2018). This selectiveness in adopting technology begs the question of what factors could make the UAE embrace or accept new technologies, including AI-based cybersecurity systems. One of the probable reasons for the slow adoption and use of AI in cybersecurity systems in UAE organizations is the employees' perception and attitudes towards such intelligent technologies. Research shows that employees tend to resist digital technology consciously or unconsciously if they perceive such a technology to be a threat to their jobs or positions (Bhargava et al., 2021; K. Nam et al., 2021; Tabrizi et al., 2019). K. Nam et al. (2021) asserted that perceived job insecurity is a significant hindrance to the adoption of technology, while Bhargava et al. (2021) argued that, though humans and AI will have to work hand in hand, the majority of employees perceive such technologies as a threat and not as an opportunity. Pertaining to attitudes, Losova (2014) argued that the decision to use a technology or system depends on the extent to which the user likes or dislikes it based on their perceptions. This implies that users are likely to embrace or use technology if they perceive it to be beneficial, helpful, or pleasant and reject it if they perceive it to be harmful, unpleasant, or destructive.

Research shows that user acceptance and attitude play a fundamental role in adopting and implementing digital technologies such as AI-based cybersecurity systems (Chaudhry, 2018; Ngeno et al., 2021; Taherdoost, 2019; Taherdoost et al., 2012). Studies show that a potential user's acceptance of technology can be influenced or explained by factors such as ease of use, usefulness, and self-efficacy, among others (Hoong et al., 2017; Lai, 2017). In line with these observations, scholars have derived several theoretical models that explain or predict the various factors associated with user acceptance of digital technology. Some of these models include the task-technology fit (TTF) model, the protection motivation theory (PMT), the unified theory of acceptance and use of technology (UTAUT) model, and the technology acceptance model (TAM). Some of these models have closely related features or aspects; for example, TAM's perceived usefulness, PMT's perceived response efficacy, and UTAUT's performance expectancy (H. J. Lee et al., 2018; Sari et al., 2019).

Even though the above theoretical models have been widely used to explain users' behavior toward technologies, doubts still exist over their ability to explain and predict the acceptance of some of the complex modern technologies, such as AI-based cybersecurity systems, which people have little or no knowledge about. Lu et al. (2019) asserted that some of the components in some of the above theoretical models are not relevant or applicable to the current emerging technologies such as AI, which exhibit human-like intelligence. According to Lu et al. (2019), most of the above theoretical models were designed for emerging non-intelligent technologies. In particular, Liu and colleagues observed that perceived usefulness and ease of use, which are some of the inherent constructs in the existing theories, were irrelevant and ineffective in predicting users' willingness to adopt AI technology because AI-based devices do not necessarily need users to learn how to use them but are instead designed to consciously or unconsciously interact with users like real human beings (Gursoy et al., 2019; Lu et al., 2019).

Therefore, there is a need for further research on intelligent technologies to develop comprehensive models that delineate the psychological pathway to users' intention or willingness to adopt such technologies. So far, there is scarce technology acceptance research covering the multi-faceted role of intelligent technologies. Besides, the few studies conducted in this area are entirely based on the existing technology acceptance theories, making it difficult to explain and predict factors contributing to the slower adoption rate of AI-based cybersecurity systems in the public sector compared to other emerging technologies. This research gap warranted conducting research that would empirically determine such factors.

Therefore, the present research adopts and extends the existing technology acceptance theories, especially the Protection Motivation Theory (PMT). It extends this theory by adding two new constructs, job insecurity (JI) and resistance to change (RTC), as significant factors determining the intention to adopt AI cybersecurity systems. The rationale for this extension was the finding that previous studies have linked job insecurity with resistance to change, especially when digital technologies are involved. As previously indicated in this section, research has shown that employees tend to resist digital technology consciously or unconsciously if they perceive such a technology to be a threat to their jobs or positions (Bhargava et al., 2021; K. Nam et al., 2021; Tabrizi et al., 2019). K. Nam et al. (2021) asserted that perceived job insecurity is a significant hindrance to the adoption of technology, while Bhargava et al. (2021) argued that, though humans and AI will have to work hand in hand, the majority of employees perceive such technologies as a threat and not as an opportunity. Against this background, the two constructs (job insecurity and resistance to change) were identified as possible factors that could affect the intention to adopt AI-based cybersecurity systems in the UAE, hence their inclusion in the extended model. While previous studies have attempted to expand PMT and integrate it with other models, none of these studies had integrated job insecurity and resistance to change constructs at the time of writing this research article. Therefore, by combining the two constructs into the original PMT model, the study expands the available body of knowledge on technology by demonstrating that job insecurity and resistance to change can significantly influence acceptance or willingness to adopt intelligent technologies such as AI-based cybersecurity systems.

LITERATURE REVIEW

As mentioned earlier, scholars have proposed different innovation models, which include the Unified Theory of Acceptance and Use of Technology (UTAUT), Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Theory of Reasoned Action (TRA), and the Technology Adoption Model (TAM). Most of these theories are quantitative and seek to enlighten organizations on who is more or less likely to adopt a technological innovation in an organization. After critically reviewing the above models and considering the context of the research topic, the Protection Motivation Theory (PMT) emerged as the most applicable and relevant theoretical model for the present study. The selection criteria included the research problem, where PMT was deemed the most suitable for a cybersecurity-related study. However, as mentioned earlier, the model was expanded by introducing two constructs, job insecurity and resistance to change, to enhance its relevance and usefulness in predicting and explaining factors influencing users' intentions to adopt AI cybersecurity systems. The inclusion of these variables was also meant to address the PMT's inherent weaknesses because every model has both weaknesses and strengths.

PROTECTION MOTIVATION THEORY (PMT)

Initially developed by Ronald Rogers in 1975, the PMT model aimed to explain how people are motivated to protect themselves from various perceived health-related threats (Rogers, 1975). Rogers argued that behavioral change/intention resulting from health-related threats could be expedited by three core stimuli: the probability of threat occurrence, the magnitude of noxiousness, and recommended response efficacy. Roger's original PMT model was further improved to incorporate self-efficacy after teaming up with Maddux in 1983 (Maddux & Rogers, 1983). This was after observing that self-efficacy significantly influenced behavioral intentions. The resultant PMT model is illustrated in Figure 1.

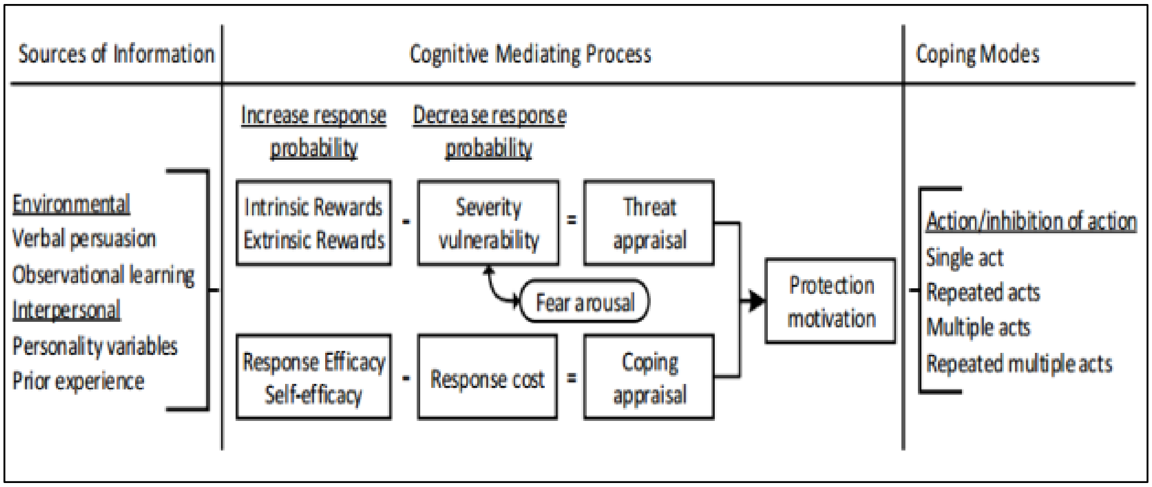

Figure 1. Protection Motivation Theory (Rogers, 1983)

As illustrated in Figure 1, the revised model included two constructs, namely threat appraisal, which was adopted from the expectancy-value model by Lazarus and Folkman (1984), and coping appraisal, adopted from Bandura's (1977) social cognitive theory. The threat appraisal entails assessing the probability of the occurrence of threats and the magnitude of the harm. As illustrated in Figure 2, threat appraisal constitutes two variables: perceived vulnerability and perceived severity. As per the PMT model in Figure 2, people respond to threats, such as a cybersecurity threat, by first assessing the extent of the danger and then evaluating how the recommended behavior can help cope with the identified threat (coping appraisals). The coping appraisal refers to the area in which an individual or organization can avoid or prevent potential harm by adopting the recommended approach/behavior (response efficacy) and the extent to which an individual can effectively implement the recommended behavior (self-efficacy) (Rogers, 1983). Therefore, in short, the PMT model suggests that behavioral intention toward the adoption of a security system depends on the threat (that is, perceived severity and perceived vulnerability) and the coping mechanisms (response efficacy and self-efficacy) (Figure 2).

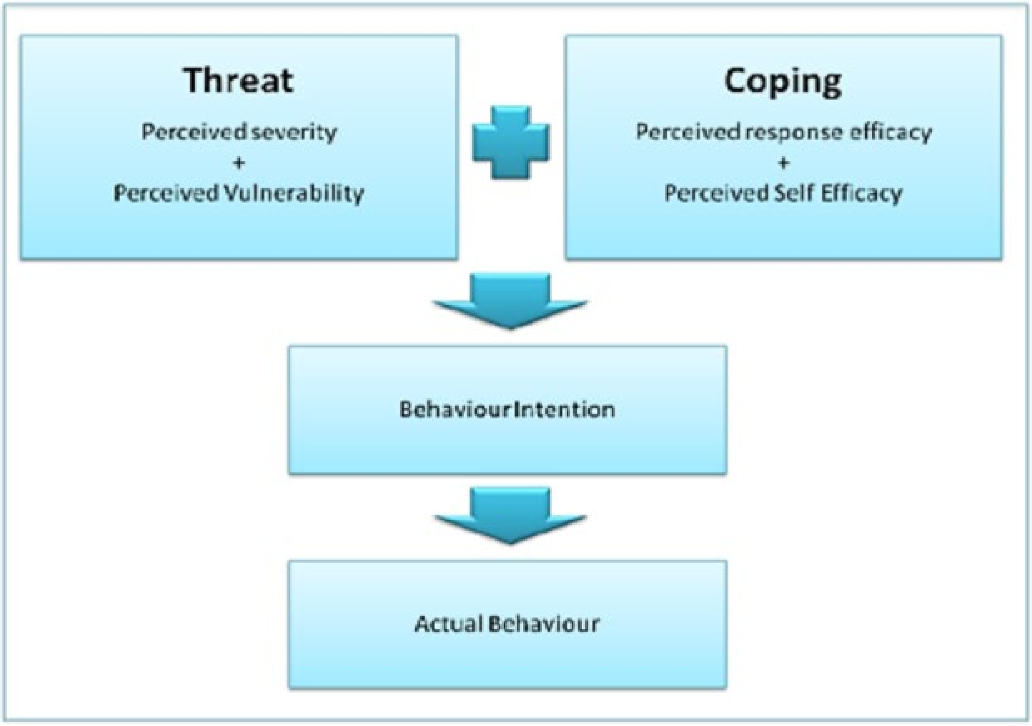

Figure 2. Protection Motivation Theory (Rogers, 1975, 1983)

RESEARCH FRAMEWORK AND HYPOTHESIS DEVELOPMENT

As mentioned above, the PMT model has been deemed the most appropriate theoretical base for the present study. This decision was based on a comprehensive review of the research problem, relevant literature, and the available technological acceptance models. PMT model has also been widely applied in various studies, particularly those focusing on adopting information security technologies (for example, Chenoweth et al., 2009; Ifinedo, 2012; Y. Lee, 2011; Meso et al., 2013; H. Y. S. Tsai et al., 2016). It is worth noting that the model's primary focus is on predicting how individuals respond to threats, thus making it relevant to the current study, which is dealing with a threat (cybercrimes). The model suggests that behavioral intention towards the adoption of a security system depends on the threat (that is, perceived severity and perceived vulnerability) and the coping mechanisms (response efficacy and self-efficacy). However, due to the nature of the research topic, the PMT model was extended to enhance its predictive power by including two additional variables: job insecurity and resistance to change. Though a few studies have developed this model to improve its explanatory or predictive power – for example, Lee (2011) extended the model by including social influences, moral obligation, and actual control variables – none of the previous studies had extended this model by including job insecurity and resistance to change variables. Figure 3 illustrates the research framework used in the present study.

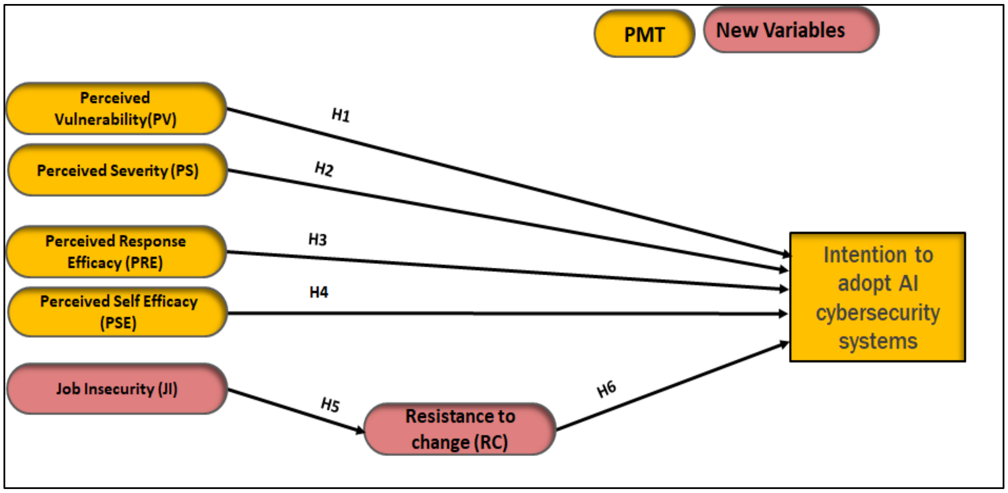
PMT
New Variables
Perceived Vulnerability(PV)
Perceived Severity (PS)
Perceived Response Efficacy (PRE)
Perceived Self Efficacy (PSE)
Job Insecurity (JI)
Resistance to change (RC)
Intention to adopt AI cybersecurity systems
H1
H2
H3
H4
H5
H6

Figure 3. Research framework

As illustrated in Figure 3, the research framework for the present study comprised six variables whose effect on the intention to adopt AI cybersecurity systems was tested using seven hypotheses. The six variables included Perceived Vulnerability (PV), Perceived Severity (PS), Perceived Response Efficacy (PRE), and Perceived Self Efficacy (PSE), which were derived from the PMT model, and Job Insecurity (JI) and Resistance to Change (RTC), which were added to the model to enhance its effectiveness in predicting and explaining users' intention to adopt AI cybersecurity systems. These variables and associated hypotheses are critically discussed below.

Perceived Vulnerability (PV)

PV refers to the extent to which a person believes they are likely to experience or face a threat (C.-Y. Huang & Kao, 2015; Rogers, 1983). The PMT suggests that an individual's perceived vulnerability is directly related to their intention to adopt the recommended coping response. This implies that users are likely to comply with the recommended security guidelines or other security measures if they believe they can be attacked. However, studies have reported mixed findings regarding this relationship. For instance, studies by Nguyen (2013) and Mwagwabi (2015), which focused on health-related threats, established that the perceived vulnerability and the intention to undertake a recommended action are not directly related. Nguyen (2013) found that perceived vulnerability did not predict the choice to give vitamin supplements but instead had a moderating effect on the relationship between perceived benefits and the need to administer vitamin supplements. Closely related findings were also reported in a meta-analysis by Sommestad et al. (2015), which also established a weak relationship between the two variables. In support of these findings, Williams and Joinson (2020) asserted that people tend to have low perceptions of information security as they believe that the information, they hold is not valuable enough to be targeted by cybercriminals. Another study by Liang and Xue (2010) observed an indirect relationship between the two, whereby the perceived threat was found to mediate this relationship. Even though these mixed findings raise questions on the applicability and relevance of the PMT in information security research, it seems that the perceived vulnerability of cyber attacks can significantly influence users' intention to adopt AI-based cybersecurity systems. In this regard, it was hypothesized that:

> **H1: Perceived vulnerability (PV) positively influences intention to adopt AI cybersecurity systems.**

Perceived Severity (PS)

PS refers to the extent to which a person believes a threat's consequences would be severe. According to the PMT, individuals with high perceptions of the severity of threats are more likely to comply with the coping guidelines. This relationship has been confirmed by several information security studies, such as Jenkins et al. (2014), Y. Lee and Larsen (2009), and Wong et al. (2016), which established that perceived severity significantly influenced users' intention to adhere to the recommended guidelines. Similar findings have also been reported in health-related studies (e.g., Abubakar & Ahmad, 2013; C.-Y. Huang & Kao, 2015; Yu, 2012), whereby perceived severity was found to influence users' intention to perform the recommended behavior significantly. Nonetheless, a study by Wang (2020) presented contradictory findings whereby the perceived severity of using debit and credit cards had an insignificant impact on users' intention to adopt mobile payment. Despite such contradictory results, most studies in health and information security have shown that perceived severity enhances users' intention to adopt AI cybersecurity systems. Therefore, it was hypothesized that:

> **H2: The perceived severity (PS) positively influences the intention to adopt AI cybersecurity systems.**

Perceived Response Efficacy (PRE)

PRE is the perceived effectiveness of the recommended coping strategy in preventing or avoiding a threat (Hanus & Wu, 2016; Rogers, 1975). In information security systems, response efficiency refers to the level of confidence among users that adopting a particular security system or feature would prevent a security threat from occurring. A large body of the available literature has demonstrated that response efficacy is a critical factor in the determination of users' intention to adopt a technology (Hanus & Wu, 2016; Johnston & Warkentin, 2010; Park & Lee, 2014). For instance, response efficacy was found to significantly influence users' compliance with desktop security behavior intentions (Hanus & Wu, 2016) and intent purposely with security policy (Johnston & Warkentin, 2010). Based on these findings, the following hypothesis was formulated:

> **H3: Perceived response efficacy (PRE) positively influences the intention to adopt AI cybersecurity systems.**

Perceived Self-Efficacy (PSE)

Self-efficacy is defined as the belief in one's ability to accomplish a particular task (C.-Y. Huang & Kao, 2015; Rogers, 1983). In the context of the present study, self-efficacy entails an individual's belief that they can effectively use AI cybersecurity systems to address or cope with a cybersecurity threat. C.-Y. Huang and Kao (2015) defined self-efficacy using three dimensions, namely, strength (level of confidence attached to the system), magnitude (the extent to which an individual believes that the system will help them accomplish the task), and generalization (perception of an individual's ability to use the system to accomplish a given task). The available body of literature has shown that individuals proficient in particular computer systems are more likely to embrace or accept new technologies than the less proficient ones. For instance, self-efficacy was found to influence users' intention to embrace virus protection behaviors (D. Lee et al., 2008), adopt required security protocols on the internet (Anderson & Agarwal, 2010), and comply with set security policies and behaviors (Hanus & Wu, 2016; Johnston & Warkentin, 2010; Park & Lee, 2014). Based on these observations, it was anticipated that users who are proficient and confident in their ability to work with AI cybersecurity systems would show more interest or intention to embrace such systems, as hypothesized below:

> **H4: Perceived self-efficacy (PSE) positively influences the intention to adopt AI cybersecurity systems.**

Job Insecurity

Job insecurity is the fear of losing a job, influence, or power at the workplace because of new changes that have been introduced. Studies have shown that job insecurity has been one of the reasons why employees have been hesitant or even opposed to the adoption of new technologies in the workplace (Eren et al., 2020). According to Eren et al. (2020), research has also shown that job insecurity significantly influences users' intention to adopt new technologies through resistance to change. For instance, T. Nam (2019) indicated that job insecurity triggers resistance to change and a sense of withdrawal response among employees. Also, Feng et al. (2021), in their qualitative study, observed that job insecurity and loss of status in the organization due to the introduction of new technologies were among the main causes of employees' resistance to organizational changes. The study established that employees were more likely to resist technological or administrative changes that would reduce their positions in organizations or render their jobs obsolete. In such a scenario, the employees can resist the change by quitting or resigning, withdrawing support, and ruining the organization's reputation (Feng et al., 2021). In this regard, it was hypothesized that:

> **H5: Job insecurity is positively related to users' resistance to AI cybersecurity systems adoption.**

Resistance to Change (RTC)

RTC is the general disapproval of a change because of its adverse effects on the actor. The available body of literature has shown that RTC is a significant determinant of the intention to adopt new technology. For instance, T. H. Tsai et al. (2020) observed that new technology creates technology anxiety among users, which could ultimately lead to resistance to change because of uncertainties about the latest technology and fears of making irreversible mistakes during the implementation. However, factors such as age and experience also played a significant role, as established by Guo et al. (2013). Guo et al. (2013), in their study that examined the use of mobile health services among adults, established that older adults are more reluctant to use this technology due to heightened levels of technology anxiety. Therefore, the findings from the above studies suggest that resistance to change negatively impacts the targeted users' perception of the new technology and intention to adopt it. In this regard, the following hypothesis was formulated:

> **H6: Resistance to change (RTC) negatively influences users' intention to adopt AI cybersecurity systems.**

Materials and Methods

The study adopted a quantitative approach guided by the positivist research philosophy. The rationale for this quantitative approach was its suitability to establish the causal relationship between the different variables/constructs using the relevant statistical models and computer programs. The quantitative approach (correlational research design) allowed the researcher to test the developed research model (extended PMT) and associated research hypotheses to establish whether the identified constructs/factors influence the intention to adopt AI cybersecurity systems. In this regard, data were collected through web-based/online questionnaires divided into two parts. The first part collected the demographic information of the participants while the second part collected data relating to the six variables/constructs and the six hypotheses tested in the study. A purposive sampling technique was employed to select and recruit the participants because the researcher wanted the study population to include persons working in the IT department and/or responsible for the cybersecurity of government and semi-government organizations in the UAE. This population was preferred because the UAE government and semi-government organizations are some of the primary targets for cybercriminals (Al-Khater et al., 2020). They are also quick to embrace new technologies though they have been slow in embracing AI-based cybersecurity frameworks (Editor's Desk, 2020; Malek, 2018; Wilson, 2020). Through this approach, the researcher recruited 370 respondents, with 340 of them responding, a response rate of 91.9%. The sample size was initially supposed to be 178 based on the general power (G*Power) analysis software, but since it was impossible to get a 100% response rate, the number was increased to accommodate the likelihood of unreturned or incomplete questionnaires.

For each construct in the questionnaire, a series of statements developed from the existing literature but customized to fit the research topic was provided, from which the respondents were required to indicate the level of agreement with each statement using a 5-point or 7-point Likert scale, depending on the construct being examined (see Appendix). Combining the 5-point and 7-point Likert scales in this study helped to minimize the common method variance/bias (Lin et al., 2015). The collected data was analyzed through the PLS-SEM strategy using SmartPLS software. The analysis entailed two major phases. The first phase assessed the measurement model, whereby the internal consistency validity, indicator reliability, convergent validity, and discriminant validity were determined. These metrics were adopted from previous research and their use in the present study was based on Hair et al.'s (2016) finding that they are the most critical metrics for evaluating the measurement model. The second phase of analysis entailed assessing the structural model. Here, the SmartPLS software was used to determine the structural relationships between the variables and constructs and test the hypotheses formulated. The structural model analyses included lateral collinearity, path coefficients, coefficient of determination (R2 value), F2-effect size, and predictive relevance (Stone-Geisser's Q2).

DATA ANALYSIS AND RESULTS

PROFILE OF RESPONDENTS

The five demographic characteristics considered in the study were age, gender, occupation, job levels, and educational background. Research has shown that these demographic characteristics can influence people's behavior, perception, and attitudes, and hence, their intention to adopt new technologies in their organizations. For instance, Morris et al. (2005) observed that gender, occupational, and job levels affect individual use and adoption of technology. Their study established that the effects of gender on the adoption and use of technology were more pronounced among older employees than young employees. This finding implied that age and gender could determine how individuals adopt new technology. Pertaining to education level, another study by Baker et al. (2007) demonstrated that the higher the level of education, the more the likelihood of embracing or adopting a technology. The researchers observed that more highly educated individuals get more training and greater exposure to IT as part of their education and are more likely to adopt new technologies. Therefore, owing to the significant role the above demographic characteristics play in determining an individual's decision to adopt or embrace a technological innovation, it was imperative to capture them to understand whether they have any influence on the intention to use AI-based cybersecurity systems. In this regard, Table 1 presents the demographic characteristics of the research participants.

As Table 1 shows, most respondents were employees at government or semi-government organizations (87.4%), while the rest were outsourced employees working for the government (12.6%). Regarding their age, most of them (66.5%) were aged 21-30 years, followed by 31-40 years (23.8%) and 41-50 years (6.5%). Only 3.2% of the respondents were aged above 51-60 years. Male respondents were the majority (52.9%). In terms of academic achievements, most respondents (89.1.8%) had a bachelor's degree, followed by a Master's degree (7.1%). Those with a Doctor's degree were only 3.8%. Most respondents (67.9%) were from the middle level, followed by the senior level (22.4%). Those in junior levels were only 9.7% (Table 1).

Table 1. Respondent demographic data

		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	*Female*	160	47.1	47.1	47.1
	Male	180	52.9	52.9	100.0
	Total	340	100.0	100.0	
Age	*21 – 30 years old*	226	66.5	66.5	66.5
	31 –40 years old	81	23.8	23.8	90.3
	41 –50 years old	22	6.5	6.5	96.8
	51 – 60 years old	11	3.2	3.2	100.0
	Total	340	100.0	100.0	
Occupation	*Government employees*	125	36.8	36.8	36.8
	Semi-government employees	172	50.6	50.6	87.4
	Outsourced employees working in government	43	12.6	12.6	100.0
	Total	340	100.0	100.0	
Educational level	*Bachelor's degree*	303	89.1	89.1	89.1
	Master's degree	24	7.1	7.1	96.2
	Doctor's degree	13	3.8	3.8	100.0
	Total	340	100.0	100.0	
Job level	*Junior level*	33	9.7	9.7	9.7
	Middle level	231	67.9	67.9	77.6
	Senior level	76	22.4	22.4	90.3
	Total	340	100.0	100.0	

Common Method Variance (CMV) Test

Research shows that common method variance (CMV) can inflate or deflate findings, leading to erroneous findings (Craighead et al., 2011). To this end, the marker variable model and baseline model were used to determine the presence of CMV in the path model, as shown in Table 2. A comparison of the two models shows that the percentage increase of R^2 of the dependent variables (Intention to Adopt (ITA) and Resistance to Change (RC)) was 2.3 and 0.0, respectively, after the introduction of the marker variable into the path model. This increase was below the 10% increase recommended by Lindell and Whitney (2001) as the indicator of CMV. For this reason, the presence of CMV in the path model used was overruled.

Table 2. Common Method Variance (CMV) test

Variable	R^2 -Baseline model	R^2 -Marker Variable Model	% changes
Intention to Adopt	**0.644**	**0.659**	2.3%
Resistance to Change	**0.107**	**0.107**	0.0%

Assessment of the Measurement Model

As mentioned in the previous section, the first stage in the PLS-SEM analysis involved the assessment of the outer/measurement model to understand the relationship between indicators and their constructs. The measurement model tested the reliability and validity of the instruments used based on the guidelines suggested by Hair et al. (2019) and Ramayah et al. (2018), whereby parameters such as convergent validity and discriminant validity were used.

Convergent Validity

Convergent validity describes the extent to which various construct indicators agree. It is the extent to which a construct converges to explain its indicators’ variance (Hair et al., 2021). The convergent validity was tested using the average variance extracted (AVE) for all construct indicators, as Hair et al. (2021) suggested. The AVE was obtained by dividing the sum of the squared loadings by the number of indicators associated with each construct, which means that AVE depicts a construct’s commonality (Hair et al., 2021). The threshold value of AVE is 0.50 because values above this threshold show that the construct can explain more than half of the variance of the indicators constituting the construct (Hair et al., 2021). As shown in Table 1, the AVE values were above 0.655 (when rounded off), which is above the minimum acceptable AVE of 0.50 recommended by researchers. The composite reliability (CR) ranged between 0.85 and 0.94, exceeding the minimum value of 0.7.

Table 3. Convergent validity

Variable	Item	Loading	CR	AVE
Intention to Adopt (ITA)	ITA01	0.884	0.915	0.782
	ITA02	0.889		
	ITA03	0.879		
Job Insecurity (JI)	JI01	0.921	0.931	0.819
	JI02	0.900		
	JI03	0.894		
Perceived Response Efficacy (PRE)	PRE01	0.840	0.885	0.719
	PRE02	0.817		
	PRE03	0.886		
Perceived Self Efficacy (PSE)	PS01	0.882	0.851	0.655
	PS02	0.870		
	PS03	0.863		
Perceived Severity (PS)	PSE01	0.774	0.905	0.760
	PSE02	0.798		
	PSE03	0.854		
Perceived Vulnerability (PV)	PV01	0.905	0.923	0.801
	PV02	0.890		
	PV03	0.889		
Resistance to Change (RC)	RC01	0.908	0.937	0.789
	RCO2	0.868		
	RCO3	0.885		
	RCO4	0.892		

Discriminant Validity

Discriminant validity determines the empirical distinctiveness of a construct from other constructs utilized in the structural model (Hair et al., 2021). One of the metrics used to measure discriminant validity is Fornell and Larcker's (1981) metric, which involves comparing each construct's AVE (squared variance within) with the squared inter-construct correlation (shared variance between constructs) of that same construct and all other constructs making up the model. In this metric, each construct's AVE should be larger than the shared variance between all model constructs (Hair et al., 2021) (Table 4).

Table 4. Discriminant validity (Fornell & Larcker criterion)

	AIK	JI	PRE	PSE	PS	PV	RC
AIK	0.884						
JI	-0.071	0.905					
PRE	0.496	-0.007	0.848				
PSE	0.685	0.010	0.460	0.809			
PS	0.679	-0.019	0.387	0.593	0.872		
PV	0.653	0.000	0.456	0.565	0.593	0.895	
RC	-0.125	0.327	0.019	-0.042	-0.157	0.028	0.888

Note: ITA = Intention to Adopt, JI = Job Insecurity, PRE = Perceived Response Efficacy, PS = Perceived Severity, PSE = Perceived Self Efficacy, PV = Perceived Vulnerability, RC = Resistance to Change.

While the Fornell-Larcker criterion has been the traditional metric for discriminant validity, recent research shows that this measure is inaccurate. For instance, Henseler et al. (2015) indicated that the Fornell-Larcker criterion does not reliably determine discriminant validity in contexts where there is a slight difference in the indicator loadings of a construct (for example, between 0.65 and 0.85). Therefore, the researcher also utilized the heterotrait–monotrait ratio (HTMT) of correlations suggested by Hair et al. (2021) and Henseler et al. (2015) to test the discriminant validity. Based on this criterion, the threshold value for discriminant validity is ≤0.90 for structural models whose constructs are theoretically similar; values above 0.90 indicate the absence of discriminant validity. However, if the constructs are theoretically different, a lower threshold value of ≤0.85 is acceptable (Hair et al., 2021; Henseler et al., 2015). As shown in Table 5, the values of HTMT were all lower than the threshold value of ≤ 0.90 (for theoretically different constructs); the highest HTMT value was 0.860, which was far below the threshold mentioned above. As such, the researcher concluded that the respondents understood that the nine constructs utilized in the present study were distinct.

Table 5. Discriminant validity (HTMT criterion)

	AIK	JI	PRE	PSE	PS	PV	RC
AIK							
JI	0.078						
PRE	0.594	0.081					
PSE	0.860	0.097	0.597				
PS	0.794	0.059	0.471	0.752			
PV	0.751	0.034	0.539	0.703	0.688		
RC	0.135	0.351	0.032	0.064	0.177	0.036	

Note: ITA = Intention to Adopt, JI = Job Insecurity, PRE = Perceived Response Efficacy, PS = Perceived Severity, PSE = Perceived Self Efficacy, PV = Perceived Vulnerability, RC = Resistance to Change.

Lateral Collinearity

According to Hair et al. (2021), lateral collinearity issues in the structural model regressions are examined to avoid method biases. In this regard, the researcher regressed all variables against a common variable to determine the variance inflation factor (VIF) values, which are used to determine the presence of collinearity. Hair et al. (2021) argued that VIF values above 5 depict possible collinearity issues among the predictor variables. However, Table 6 shows that the VIF values for all constructs were less than 3, suggesting that no bias or collinearity was involved, despite data coming from a single source.

Table 6. Collinearity testing

Predictors	Variance Inflation Factor (VIF)	
	Intention to Adopt (ITA)	Resistance to Change (RC)
Job Insecurity (JI)		1.000
Perceived Response Efficacy (PRE)	1.374	
Perceived Self Efficacy (PSE)	1.829	
Perceived Severity (PS)	1.903	
Perceived Vulnerability (PV)	1.853	
Resistance to Change (RC)	1.051	

Path Coefficients

Path coefficients help to understand the causal linkages/relationships among the constructs; they indicate how changes in the values of an endogenous construct associate with a specific predictor construct when all other predictor constructs are kept constant (Hair et al., 2021). In PLS-SEM, the significance of path coefficients is assessed by bootstrapping the standard errors to determine path coefficients' t-values or confidence intervals. A path coefficient is considered significant at a 5% level if value 0 does not fall into the 95% confidence interval (Hair et al., 2021). On the other hand, path coefficients are considered relevant if they lie between -1 and +1; values closer to -1 depict a strong negative relationship, while those closer to +1 show a strong positive relationship (Hair et al., 2021). It is worth noting that values below -1 and above +1 are unacceptable because they depict the presence of multicollinearity, thus necessitating the implementation of multicollinearity reduction methods to address the biases. In the present study, the path coefficients, standard errors, t-values, and p-values for the structural model were reported using a 5,000-sample re-sample bootstrapping procedure (Table 7).

Table 7. Direct hypothesis results

Hypothesis	Relationships	std.Beta	std.Dev	T- value	P- value	BCI LL	BCI UL	Decision
H1	PV à ITA	0.253	0.058	4.343	*p*<.001	0.137	0.364	Accepted
H2	PS à ITA	0.282	0.060	4.674	*p*<.001	0.164	0.396	Accepted
H3	PRE à ITA	0.130	0.053	2.437	0.015	0.028	0.240	Accepted
H4	PSE à ITA	0.312	0.069	4.556	*p*<.001	0.184	0.450	Accepted
H5	JI à RC	0.327	0.049	6.620	*p*<.001	0.234	0.428	Accepted
H6	RC à ITA	-0.077	0.029	2.613	0.009	-0.134	-0.019	Accepted

Note: ITA = Intention to Adopt, JI = Job Insecurity, PRE = Perceived Response Efficacy, PS = Perceived Severity, PSE = Perceived Self Efficacy, PV = Perceived Vulnerability, RC = Resistance to Change.

With a path coefficient of t= 4.343 (β= 0.253, p< 0.001), Perceived Vulnerability was found to be a statistically significant predictor of the intention to use AI cybersecurity systems. Therefore, H1 was accepted. H2 was also accepted because a significant and positive relationship was established between PS and ITA t= 4.674 (β = 0.282, p< 0.001). The relationship between PRE and ITA was found to be positive and significant, t = 2.437 (β = 0.130, p<0.015), thus supporting H3. A significant positive relationship was also established between PSE and ITA, t = 4.556 (β = 0.312 and p<0.001), implying that H4 was supported. H5 proposed a positive relationship between JI and ITA, and the findings supported it because the path coefficients were t = 6.620 (β = 0.327, p<0.001). Finally, RC and ITA were found to be negatively related, t = 2.613 (β = -0.077, p<0.009), hence supporting H6 (Figure 4).

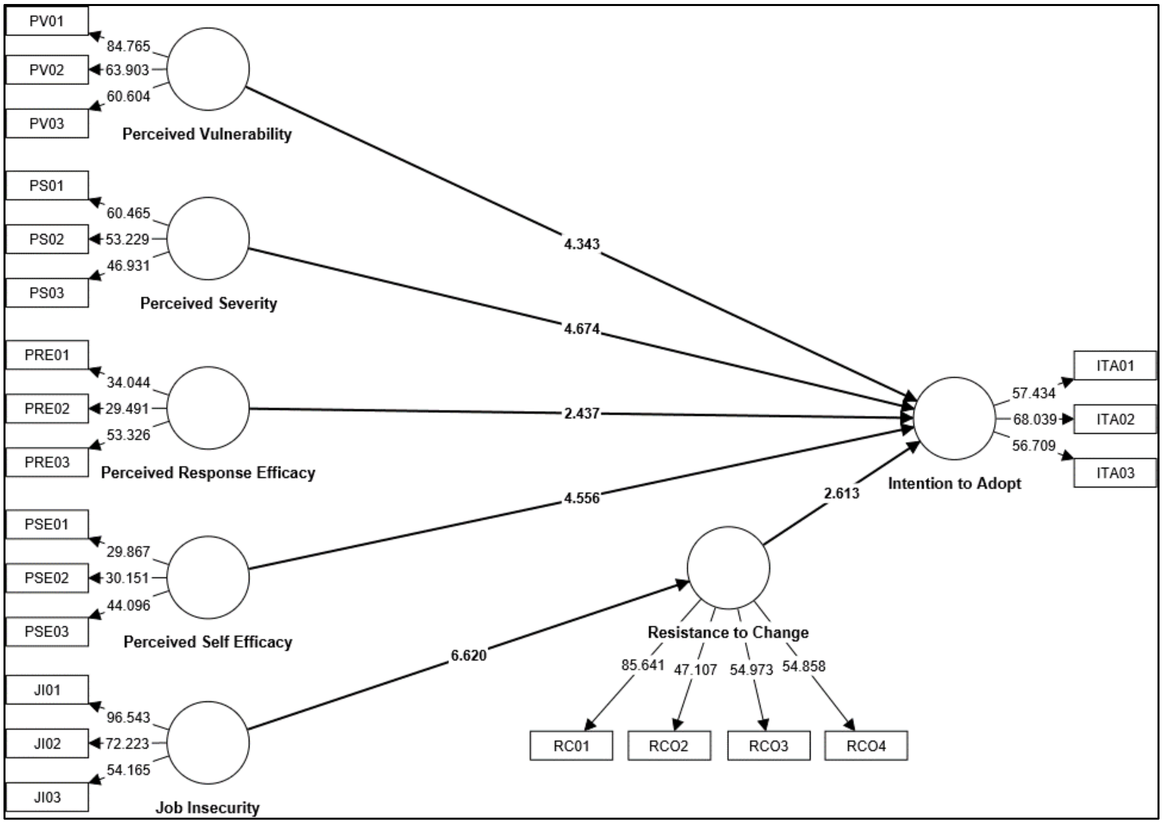

Figure 4. PLS Structure Model

R^2-Coefficient of Determination

The coefficient of determination R^2 was examined to determine the model's explanatory/in-sample predictive power. Shmueli and Koppius (2011) found that R^2 values range between 0 and 1, and the closer the value is to 1, the greater the explanatory power. On the other hand, Hair et al. (2011) grouped R^2 values into weak (0.25), moderate (0.50), and substantial (0.75). However, some methodology scholars assert that acceptable R^2 values depend heavily on the research context (Raithel et al., 2012). To this end, an R^2 value of as low as 0.10 can be considered satisfactory, depending on the type of research. Table 8 shows that the R^2 values for the intention to adopt and resistance to change were (0.644) and (0.107), respectively. One of these values (0.644) can be considered substantial, while the other (0.107) can be considered weak based on Hair et al.'s classification.

Table 8. R^2 Coefficient of determination

	R-square	**Explanatory Power (R^2)**	
		Chin (1998)	Cohen (1988)
Intention to Adopt	0.644	**0.768** **(Substantial)**	0.768 (Substantial)
Resistance to Change	0.107	**0.107** **(Weak)**	0.107 (Moderate)

Effect Size f^2

Although the effect size (f^2) is not a requirement, Hair et al. (2021) noted that it can provide an alternative perspective on the findings. Hair and colleagues categorized f^2 into small effect (0.02), medium effect (0.15), and large effect (0.35) and argued that the larger the effect size, the stronger the relationship between the two variables. As shown in Table 9, the f^2 effect size of all constructs ranged from small to medium, implying that the constructs depicted moderate relationships.

Table 9. f^2 effect size

Hypothesis	Relationships	Effect Size		Explanatory Power (R^2)	
		f^2	Magnitude	Chin (1998)	Cohen (1988)
H1	PV -> ITA	0.097	**Small**	0.644 (Substantial)	0.644 (Substantial)
H2	PS -> ITA	0.117	**Small**		
H3	PRE -> ITA	0.034	**Small**		
H4	PSE -> ITA	0.150	**Small**		
H5	JI -> RC	0.120	**Small**		
H6	RC -> ITA	0.016	**No Effect**	0.107 (Weak)	0.107 (Moderate)

Discussion and Implications

Discussion

The above results show that factors such as perceived vulnerability, perceived severity, perceived self-efficiency, and perceived response efficacy significantly and positively influenced users' intention to adopt AI cybersecurity systems. However, job insecurity and resistance to change were found to have negatively affected the users' intention to accept and adopt AI cybersecurity technology. Similar findings have been made in many previous studies, including Al-Emran et al. (2021), Upadhyay et al. (2022), Giwah et al. (2020), G. Huang and Ren (2020), T. H. Tsai et al. (2020), and Stettner (2018). To this end, creating awareness about computer systems' vulnerability to cybercrimes and the severity of attacks can improve the acceptability and intention to adopt AI-based cybersecurity systems. These findings also suggest that when these systems are efficient and the target users feel they can use them to accomplish a specific task, the likelihood of accepting and adopting them is significantly high. Therefore, this study promotes an understanding of the factors possibly contributing to the sluggish adoption of AI cybersecurity systems in the UAE. It acts as an eye-opener for these organizations to critically evaluate themselves and establish their level of preparedness in terms of adopting AI-based cybersecurity systems and come up with measures and approaches they can adopt to minimize employees' resistance to new technological changes in cybersecurity sectors.

THEORETICAL IMPLICATIONS

The study is based on the PMT (Protection Motivation Theory) framework, widely used in information security research. However, it extends this model by including two more variables – job insecurity and resistance to change – to enhance its predictive/exploratory power. Thus, this research improves PMT and contributes to the body of knowledge on technology acceptance, especially in intelligent cybersecurity technology. The study's findings also enrich the available literature on technology adoption, considering that AI cybersecurity systems are new to many organizations and employees in the UAE, and much of the information is available from non-scholarly sources.

PRACTICAL IMPLICATIONS

By exposing the factors promoting or hindering the acceptability and adoption of AI-based cybersecurity systems, this study brings new insights into how cyber-security defense can be strengthened, thus saving individuals, businesses, and the government a lot of money. Its findings highlight the importance of creating awareness and imparting employees with the appropriate skills and knowledge to improve perceived self-efficacy and perceived response efficacy. They also indicate that organizations should embrace measures that reduce job insecurity and resistance to change because the two factors were found to have a negative impact on the users' intention to use AI-based cybersecurity systems.

CONCLUSION

This study's primary objective was to investigate factors influencing users' intention to adopt AI-based cybersecurity systems in the UAE. The rationale for conducting the study was the finding that the UAE has witnessed a slow adoption of AI cybersecurity systems despite being among the top countries that have embraced technologies and emerging trends such as blockchain technology, robotic process automation, and intelligent automation. It has also been established that cybersecurity threats are becoming more complex, and UAE is a significant target for cyber-attacks, thus indicating the need for a study to understand the factors contributing to the slow adoption. The study is based on the extended PMT model, whereby the influence of constructs such as PV, PS, PRE, PSE, JI, and RC on the intention to adopt AI-based cybersecurity systems in the UAE was examined. PV, PS, PRE, and PSE significantly and positively influenced users' intention to adopt AI cybersecurity systems, while JI and RC had negative impacts. These findings suggest that organizations can boost the acceptability and adoption of AI-based cybersecurity systems by establishing measures to mitigate job insecurity and resistance to change and creating awareness to improve users' understanding of their systems' vulnerability, the severity of cyber-attacks, their ability to use AI-based technologies, and the response efficacy of these technologies.

LIMITATIONS AND DIRECTIONS FOR FUTURE STUDIES

The present study relied on a quantitative approach, which limited the ability to give unique insights, which might not be captured in the questionnaire. To this end, a more flexible approach that allows deeper exploration of the topic was needed. Future research should, therefore, consider integrating both quantitative and qualitative approaches (mixed method design) for in-depth and broad coverage of the research topic. The mixed method approach would allow researchers to quantify the findings and identify new unique themes, hence enriching the existing theories on intention to adopt technology at the workplace. Another limitation was that the study's scope was limited to individuals working in government and semi-government organizations in Abu Dhabi, thus reducing the generalizability of the findings. Therefore, future studies should consider expanding the scope to enhance the results' generalizability. They should also test more constructs beyond the ones tested in the present study (from the extended PMT).

REFERENCES

Abubakar, F. M., & Ahmad, H. B. (2013). The moderating effect of technology awareness on the relationship between UTAUT constructs and behavioural intention to use technology: A conceptual paper. *Australian Journal of Business and Management Research*, *3*(2), 14-23. https://doi.org/10.52283/NSWRCA.AJBMR.20130302A02

Al-Emran, M., Granić, A., Al-Sharafi, M. A., Ameen, N., & Sarrab, M. (2021). Examining the roles of students' beliefs and security concerns for using smartwatches in higher education. *Journal of Enterprise Information Management*, *34*(4), 1229-1251. https://doi.org/10.1108/JEIM-02-2020-0052

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, 137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643. https://doi.org/10.2307/25750694

Baker, E. W., Al-Gahtani, S. S., & Hubona, G. S. (2007). The effects of gender and age on new technology implementation in a developing country: Testing the Theory of Planned Behavior (TPB). *Information Technology & People*, *20*(4), 352–375. https://doi.org/10.1108/09593840710839798

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191-215. https://doi.org/10.1037/0033-295X.84.2.191

Bhargava, A., Bester, M., & Bolton, L. (2021). Employees' perceptions of the implementation of robotics, artificial intelligence, and automation (RAIA) on job satisfaction, job security, and employability. *Journal of Technology in Behavioral Science*, *6*(1), 106-113. https://doi.org/10.1007/s41347-020-00153-8

Chandra, G. R., Sharma, B. K., & Liaqat, I. A. (2019). UAE's strategy towards most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 2803-2809. https://doi.org/10.35940/ijitee.L3022.1081219

Chaudhry, S. (2018). Managing employee attitude for a successful information system implementation: A change management perspective. *Journal of International Technology and Information Management*, *27*(1), 57-90. https://doi.org/10.58729/1941-6679.1364

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences, Waikoloa, HI, USA*, 1-10.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), vii-xvi. https://www.jstor.org/stable/249674

Craighead, C. W., Ketchen, D. J., Dunn, K. S., & Hult, G. T. M. (2011). Addressing common method variance: Guidelines for survey research on information technology, operations, and supply chain management. IEEE Transactions on Engineering Management, 58(3), 578-588. https://doi.org/10.1109/TEM.2011.2136437

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates. https://doi.org/10.4324/9780203771587

DarkMatter Group. (2019). DarkMatter group calls for improved vigilance as UAE's cyber-threat landscape reaches critical level. https://www.prnewswire.com/ae/news-releases/darkmatter-group-calls-for-improved-vigilance-as-uaes-cyber-threat-landscape-reaches-critical-level-300869316.html

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21-39. https://doi.org/10.5121/ijaia.2015.6102

Editor's Desk. (2020). UAE embraces blockchain technology and digital identity to fight Covid-19! *Blockchain Magazine*. https://blockchainmagazine.net/uae-embraces-blockchain-technology-and-digital-identity-to-fight-covid-19/

Eren, A. S., Ozyasar, K., & Taşliyan, M. (2020). The effect of technology adoption on job insecurity: A case study in Turkish textile sector. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 17*(2), 1007-1023. https://doi.org/10.33437/ksusbd.706168

Feng, C., Cooper, B., & Zhu, C. J. (2021). How and when job security reduces resistance to change in the context of organizational change. *The Journal of Applied Behavioral Science*. https://doi.org/10.1177/00218863211040613

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*(3), 382-388. https://doi.org/10.2307/3150980

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2020). An empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*, *21*(2), 215-233. https://doi.org/10.1108/JIC-03-2019-0063

Guo, X., Sun, Y., Wang, N., Peng, Z., & Yan, Z. (2013). The dark side of elderly acceptance of preventive mobile health services in China. *Electronic Markets*, *23*(1), 49-61. https://doi.org/10.1007/s12525-012-0112-4

Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R. (2019). Consumers acceptance of artificially intelligent (AI) device use in service delivery. *International Journal of Information Management*, *49*, 157-169. https://doi.org/10.1016/j.ijinfomgt.2019.03.008

Guven, H. (2018). *The state of cyber (in)security in the United Arab Emirates.* http://www.cs.tufts.edu/comp/116/archive/spring2018/hguven.pdf

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). A *primer on partial least squares structural equation modeling (PLS-SEM)*. SAGE Publications. https://us.sagepub.com/en-us/nam/a-primer-on-partial-least-squares-structural-equation-modeling-pls-sem/book244583

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Evaluation of reflective measurement models. *Partial Least Squares Structural Equation Modeling (PLS-SEM) using* R (pp. 75-90). Springer. https://doi.org/10.1007/978-3-030-80519-7_4

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-151. https://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24 https://doi.org/10.1108/EBR-11-2018-0203

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Henseler, J., Ringle, C., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*, 115-135. https://doi.org/10.1007/s11747-014-0403-8

Hoong, A. L. S., Thi, L. S., & Lin, M.-H. (2017). Affective technology acceptance model: Extending technology acceptance model with positive and negative affect. In M. Mohiuddin, N. Halilem, S. M. Ahasanul Kobir, & C. Yuliang (Eds.), *Knowledge management strategies and applications* (pp. 147-165). IntechOpen. https://doi.org/10.5772/intechopen.70351

Huang, C.-Y., & Kao, Y.-S. (2015). UTAUT2 based predictions of factors influencing the technology acceptance of phablets by DNP. *Mathematical Problems in Engineering*, Article 603747. https://doi.org/10.1155/2015/603747

Huang, G., & Ren, Y. (2020). Linking technological functions of fitness mobile apps with continuance usage among Chinese users: Moderating role of exercise self-efficacy. *Computers in Human Behavior*, *103*, 151-160. https://doi.org/10.1016/j.chb.2019.09.013

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 196-213. https://doi.org/10.1080/02681102.2013.814040

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566. https://doi.org/10.2307/25750691

Lai, P. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21-38. https://doi.org/10.4301/S1807-17752017000100002

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454. https://doi.org/10.1080/01449290600879344

Lee, H. J., Roh, E. H., & Han, K. S. (2018). A study on factors of information security investment in the fourth industrial revolution. *International Journal of Advanced Science and Technology*, *111*, 157-174. https://doi.org/10.14257/ijast.2018.111.14

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. Decision Support Systems, 50(2), 361-369. https://doi.org/10.1016/j.dss.2010.07.009

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7). https://doi.org/10.17705/1jais.00232

Lin, T.-C., Huang, S.-L., & Hsu, C.-J. (2015). A dual-factor model of loyalty to IT product – The case of smartphones. *International Journal of Information Management*, *35*(2), 215-228. https://doi.org/10.1016/j.ijinfomgt.2015.01.001

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology, 86*(1), 114-121. https://doi.org/10.1037/0021-9010.86.1.114

Losova, V. (2014). *Technology acceptance model: A case of electronic health record in Estonia* [Master's dissertation, Copenhagen Business School, Copenhagen].

Lu, L., Cai, R., & Gursoy, D. (2019). Developing and validating a service robot integration willingness scale. *International Journal of Hospitality Management*, *80*, 36-51. https://doi.org/10.1016/j.ijhm.2019.01.005

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Malek, C. (2018). UAE embraces emerging technologies in education. *The Arab Weekly* https://thearabweekly.com/uae-embraces-emerging-technologies-education

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47-67. https://doi.org/10.1080/15536548.2013.10845672

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior. *IEEE Transactions on Engineering Management*, *52*(1), 69-84. https://doi.org/10.1109/TEM.2004.839967

Mwagwabi, F. (2015). *A Protection Motivation Theory approach to improving compliance with password guidelines* [Doctoral dissertation, Murdoch University, WA, Australia].

Nam, K., Dutt, C. S., Chathoth, P., Daghfous, A., & Khan, M. S. (2021). The adoption of artificial intelligence and robotics in the hotel industry: Prospects and challenges. *Electronic Markets*, *31*, 553–574. https://doi.org/10.1007/s12525-020-00442-3

Nam, T. (2019). Technology usage, expected job sustainability, and perceived job insecurity. *Technological Forecasting and Social Change, 138*, 155-165.https://doi.org/10.1016/j.techfore.2018.08.017

Ngeno, B., Mwoma, T., & Mweru, M. (2021). Teachers' attitude towards implementation of the competence-based curriculum in primary schools in Kericho County. *East African Journal of Education Studies*, *3*(1), 116-129. https://doi.org/10.37284/eajes.3.1.342

Nguyen, P. (2013). Mothers' perceived vulnerability, perceived threat and intention to administer preventive medication to their children. *Contemporary Management Research*, *9*(4), 399-418. https://doi.org/10.7903/cmr.11093

Park, C., & Lee, S.-W. (2014). A study of the user privacy protection behavior in online environment: Based on protection motivation theory. *Journal of Internet Computing and Services*, *15*(2), 59-71. https://doi.org/10.7472/jksii.2014.15.2.59

Raithel, S., Sarstedt, M., Scharf, S., & Schwaiger, M. (2012). On the value relevance of customer satisfaction. Multiple drivers and multiple markets. *Journal of the Academy of Marketing Science, 40*(4), 509–525. https://doi.org/10.1007/s11747-011-0247-4

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). *Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 3.0: An updated guide and practical guide to statistical analysis* (2nd ed.). Pearson.

Ramírez, J. M. (2017). Some criminal aspects of cybersecurity. In J. Ramírez, & L. García-Segura (Eds.), *Cyberspace* (pp. 141-151). Springer. https://doi.org/10.1007/978-3-319-54975-0_8

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty (Eds.), *Social psychophysiology* (pp. 153-176). Guilford Press.

Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020). Machine learning and deep learning techniques for cybersecurity: A review. In A. E. Hassanien, A. Azar, T. Gaber, D. Oliva, & F. Tolba (Eds.), *Proceedings of the International Conference on Artificial Intelligence and Computer Vision* (pp. 50-57). Springer. https://doi.org/10.1007/978-3-030-44289-7_5

Sari, H., Othman, M., & Al-Ghaili, A. M. (2019). A proposed conceptual framework for mobile health technology adoption among employees at workplaces in Malaysia. In F. Saeed, N. Gazem, F. Mohammed, & A. Busalim (Eds.), *Recent trends in data science and soft comput*ing (pp. 736-748). Springer. https://doi.org/10.1007/978-3-319-99007-1_68

Shmueli, G., & Koppius, O. R. (2011). Predictive analytics in information systems research. *MIS Quarterly, 35*(3), 553–572. https://doi.org/10.2307/23042796

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26-46. https://doi.org/10.4018/IJISP.2015010102

Stettner, A. (2018). Mounting a response to technological unemployment. *The Century Foundation.* https://tcf.org/content/report/mounting-response-technological-unemployment/

Tabrizi, B., Lam, E., Girard, K., & Irvin, V. (2019). Digital transformation is not about technology. *Harvard Business Review*, *13*(March).

Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and Machines*, *29*(2), 187-191. https://doi.org/10.1007/s11023-019-09504-8

Taherdoost, H. (2019). Importance of technology acceptance assessment for successful implementation and development of new technologies. *Global Journal of Engineering Sciences*, *1*(3).

Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2012). Smart card technology: Awareness and satisfaction. *Journal of Computing*, *4*(6), 128-132.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Tsai, T. H., Lin, W. Y., Chang, Y. S., Chang, P. C., & Lee, M. Y. (2020). Technology anxiety and resistance to change behavioral study of a wearable cardiac warming system using an extended TAM for older adults. PloS ONE, *15*(1), e0227270. https://doi.org/10.1371/journal.pone.0227270

Upadhyay, N., Upadhyay, S., Abed, S. S., & Dwivedi, Y. K. (2022). Consumer adoption of mobile payment services during COVID-19: Extending meta-UTAUT with perceived severity and self-efficacy. *International Journal of Bank Marketing*, *40*(5), 960-991. https://doi.org/10.1108/IJBM-06-2021-0262

Wang, S.-T. (2020). The effects of risk appraisal and coping appraisal on the adoption intention of m-payment. *International Journal of Bank Marketing*, *38*(1), 21-33. https://doi.org/10.1108/IJBM-10-2018-0272

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, *6*(1), tyaa001. https://doi.org/10.1093/cybsec/tyaa001

Wilson, G. (2020). Blue prism: UAE leaders embrace intelligent automation. *Business Chief Magazine*. https://businesschief.eu/technology/blue-prism-uae-leaders-embrace-intelligent-automation

Wong, T. S., Gaston, A., DeJesus, S., & Prapavessis, H. (2016). The utility of a protection motivation theory framework for understanding sedentary behavior. *Health Psychology and Behavioral Medicine*, *4*(1), 29-48. https://doi.org/10.1080/21642850.2015.1128333

Yu, C.-S. (2012). Factors affecting individuals to adopt mobile banking: Empirical evidence from the UTAUT model. *Journal of Electronic Commerce Research*, *13*(2), 104.

APPENDIX: SURVEY QUESTIONNAIRE

Section A: Screening Question

1. Do you work in the IT department at (System, Programming, or Network section) sections or are you responsible for cybersecurity in your organization?

● Yes (if yes, proceed to the next question)

○ No (if no, do not continue. Thank you for your time)

Section B: Demographic characteristics

Explanation: Please select the box that matches your information the most.

1. Gender:

□ 1) Male □ 2) Female

2. Age:

□ 1) Under 21 years old □ 2) 21 – 30 years old
□ 3) 31 –40 years old □ 4) 41 –50 years old
□ 5) 51 – 60 years old □ 6) More than 60 years old

3. Occupation:

□ 1) Government employee □ 2) Semi Government employee
□ 3) Outsourced Employee working in Government
□ 4) Outsourced Employee working in Semi Government □ 5) Other (Please specify) ....

4. Educational level:

❑1) High school/vocational ❑2) Bachelor's degree

❑3) Master's degree ❑4) Doctor's degree

5. Job level:

❑ 1) Junior level ❑ 2) Middle level

❑ 3) Senior level ❑ 4) Others (Please specify) ....

Section C: Factors influencing users' intention to use AI cybersecurity systems at workplaces

This section comprises 12 subsections where each section contains one variable and the items used to measure it. Kindly tick (√) the answer that you best resonate with. Once again, there are no correct and wrong answers. Be honest and realistic in your assessment.

SECTION 1: PERCEIVED VULNERABILITY (PV)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	**Disagree**	**Slightly Disagree**	**Neutral**	**Slightly Agree**	**Agree**	**Strongly Agree**
1	2	3	4	5	6	7

1.	**PERCEIVED VULNERABILITY (PV)**	1	2	3	4	5	6	7
PV01	I am at risk of losing company information or files on my office computer by cybersecurity incidents.							
PV02	It is likely that I will lose company information or files on my office computer by cybersecurity incidents.							
PV03	It is possible for me to lose company information or files on my office computer by cybersecurity incidents.							

SECTION 2: PERCEIVED SEVERITY (PS)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	**Disagree**	**Slightly Disagree**	**Neutral**	**Slightly Agree**	**Agree**	**Strongly Agree**
1	2	3	4	5	6	7

2.	**PERCEIVED SEVERITY (PS)**	1	2	3	4	5	6	7
PS01	If I suffered losing my company information as a result of cybersecurity incidents, it would be severe.							
PS02	If I suffered losing my company information as a result of cybersecurity incidents, it would be serious.							
PS03	If I suffered losing my company information as a result of cybersecurity incidents, it would be significant							

SECTION 3: PERCEIVED RESPONSE EFFICACY (PRE)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

3.	PERCEIVED RESPONSE EFFICACY (PRE)	1	2	3	4	5	6	7
PRE01	AI cybersecurity systems will work in solving cyber threat problems.							
PRE02	AI cybersecurity systems are effective in solving cyber threat problems.							
PRE03	When using AI cybersecurity systems, solving cyber threat problems is more likely to be guaranteed.							

SECTION 4: PERCEIVED SELF-EFFICACY (PS)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

4.	PERCEIVED SELF-EFFICACY (PSE)	1	2	3	4	5	6	7
PSE01	I believe that I would use AI cybersecurity systems to mitigate threats							
PSE02	I feel confident that I would be able to operate AI cybersecurity systems to mitigate threats							
PSE03	I feel confident with my ability to use AI cybersecurity systems, even without any guidelines on how to use it.							

SECTION 5: ATTITUDE TOWARDS AI SECURITY SYSTEMS (AT)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

5.	Attitude towards AI security systems (AT)	1	2	3	4	5
AT01	Adopting AI in cybersecurity is important.					
AT02	Adopting AI in cybersecurity is beneficial.					
AT03	Adopting AI in cybersecurity is helpful.					
AT04	Using AI in cybersecurity is a good idea.					
AT05	Using AI in cybersecurity is a wise idea.					

SECTION 6: EFFORT EXPECTANCY (EE)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

6.	EFFORT EXPECTANCY (EE)	1	2	3	4	5	6	7
EE01	Learning how to use AI cybersecurity systems is easy for me.							
EE02	My interaction with AI cybersecurity systems is clear and understandable.							
EE03	I find AI cybersecurity system easy to use.							
EE04	It is easy for me to become skilful at using AI cybersecurity system							

SECTION 7: Facilitating Conditions (FC)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

7.	FACILITATING CONDITIONS (FC)	1	2	3	4	5	6	7
FC01	I have the necessary resources for using AI in cybersecurity for work-related purposes in my organization.							
FC02	I have the necessary knowledge to use AI in cybersecurity for work-related purposes in my organization.							
FC03	The use of AI is compatible with other technologies that I used.							
FC04	I can get help from others whenever I have difficulties using AI in cybersecurity for work-related purposes in my organization.							

SECTION 8: AI KNOWLEDGE (AAK)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

8.	AI KNOWLEDGE (AAK)	1	2	3	4	5
AAK01:	I know pretty much about AI.					
AAK02:	I do not feel very knowledgeable about AI					
AAK03:	When it comes to AI, I really don't know a lot					

SECTION 9: JOB INSECURITY (JI)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

9.	JOB INSECURITY (JI)	1	2	3	4	5	6	7
JI01:	Using artificial intelligence security systems in the company will lead to merge some of the IT security professionals' roles which will lead to reducing the number of employees within the IT security section, that is why I feel there is a high chance that I will lose my job							
JI02:	Using artificial intelligence security systems in the company will lead to merge some of the IT security professionals' roles which will lead to reducing the number of employees within the IT security section, that is why I feel insecure about the future of my job							
JI03:	Using artificial intelligence security systems in the company will lead to merge some of the IT security professionals' roles which will lead to reducing the number of employees within the IT security section, that is why I think I might lose my job in the near future							

SECTION 10: RESISTANCE TO CHANGE (RC)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

10.	RESISTANCE TO CHANGE (RC)	1	2	3	4	5	6	7
RC01	The current cybersecurity approaches are the most effective							
RC02	Fast or radical changes regarding AI cybersecurity are unwise and dangerous.							
RC03	Making sudden changes tends to create more problems than solutions.							
RC04	Slow, gradual change helps prevent catastrophes and mistakes.							

SECTION 11: BEHAVIOURAL INTENTION (BI)

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

11.	BEHAVIORAL INTENTION (BI)	1	2	3	4	5	6	7
BI01:	I intend to use AI in cybersecurity in the future.							
BI02:	I will always try to use AI in cybersecurity in my daily life.							
BI03:	I plan to use AI in cybersecurity frequently.							

SECTION 12: MARKER VARIABLE

To what extent do you agree with the following? Kindly tick (√) the appropriate answer to the following statements.

Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
1	2	3	4	5	6	7

12.	Marker Variable (MV) (Lin et al., 2015)	1	2	3	4	5	6	7
MV01:	Once I have come to a conclusion, I'm not likely to change my mind.							
MV02:	I don't change my mind easily.							
MV03:	My views are very consistent over time.							

AUTHORS

Mohammed Rashed Mohammed Al Humaid Alneyadi is a Deputy Head of the Communications and IT Department at the Global Aerospace Logistics private company in UAE. He has 24 years of experience in the Communications and IT field. He obtained his first degree in Computer Engineering from the Florida Institute of Technology (FIT), USA, in 1999. He completed his first Master of Science in Computer Science from the New York Institute of Technology (NYIT) in UAE in 2008. He completed his second Master of Science in Information Technology (Specialization in Cyber Security) at Zayed University in UAE in 2012.

Normalini Md Kassim is currently a senior lecturer in the School of Management, at the University of Science of Malaysia, and Visiting Professor at the Management & Science University (Malaysia). She is a Technical Specialist (Ts) by the Malaysian Board of Technologists. She is also a Chartered Member of the Chartered Institute of Logistics & Transport (CMILT). Her publications have appeared in IGI Global Handbook, Procedia-Social and Behavioral Sciences (Elsevier), International Journal of Productivity and Performance Management (Emerald), Global Business Review (SAGE), Taylor and Francis, Social Indicators Research, International Journal of Communication Systems, International Journal of Enterprise Information Systems, Industrial Engineering & Management Systems, Global Business and Management Research and Springer. She has experience with industries like Maybank Berhad as a system engineer for 4 years and Hewlett Packard Singapore as Project Manager for Asia Pacific Project for 10 years. She completed her Master of Business Administration (MBA) at the University of Science, Malaysia (2005) and completed her PhD in Technology Management from the same university (2012). She has now embarked on a new research area which is smart community, smart cities, and business analytics. With experience in banking, manufacturing, communication, and the financial industry, she would like to collaborate and share her experience in technology management, business analytics, and risk management area. Her full profile can be accessed at www.som.usm.my.