Human Factors in Cybersecurity, Vol. 53, 2022, 161–175
https://doi.org/10.54941/ahfe1002693

The Impact of Technology Threat Avoidance Theory Constructs on Cybersecurity Avoidance Behaviour

Hamed Alqahtani

King Khalid University, College of Computer Science, Abha, Saudi Arabia

ABSTRACT

In the field of cybersecurity, human behaviour is considered as the weakest link. We applied gamification techniques to the development of an Augmented Reality game, CybAR, which was designed to educate users about cybersecurity in an effective and entertaining way. Technology Threat Avoidance Theory (TTAT) provided the theoretical model for understanding cybersecurity avoidance behaviour. Its constructs of perceived severity, perceived susceptibility, fear, safeguard effectiveness, self-efficacy and safeguard costs were considered as direct antecedents of cybersecurity avoidance motivation and indirect predictors of cybersecurity avoidance behaviour. The purpose of the research was to examine the role of these TTAT constructs in explaining individuals' cybersecurity avoidance behaviour. Structural equation modeling was used to analyse the relationships and test the hypotheses. A cross-sectional survey of 128 students at Macquarie University was conducted to assess the effect of the TTAT on motivation and behaviour. The results showed positive support for most of the proposed relationships, with the exception of safeguard cost on cybersecurity avoidance motivation as well as perceived susceptibility on fear construct of the threat, but safeguard cost factor positively contributed to students' cybersecurity avoidance behaviour. Coping appraisal variables (perceived effectiveness, self-efficacy) were the strongest predictors of cybersecurity avoidance behaviour, especially safeguard effectiveness. Threat severity was also a significant predictor of the fear factor.

Keywords: Cybersecurity, Human behavior, Augmented reality and technology threat avoidance theory

INTRODUCTION

Digital technology has facilitated innovation, economic growth and productivity. However, it has also led to a dramatic increase in the number of cyberattacks, which can be responsible for substantial financial losses. A recent incident in Australia, for instance, involved the loss of sensitive personal information worth tens of millions of dollars. According to a 2016 report on IT security from the SANS Institute, large organizations spend approximately 35% of their annual security budget on end-user training and awareness (Filkins, 2016).

Security professionals and researchers are devoting considerable effort to addressing human behaviour as the weakest link in cybersecurity operations, but research on the human factors in cybersecurity is still in its infancy

(Howard and Prince, 2011). Recently, the focus has shifted towards a more human-centered perspective on cybersecurity, since it is not always practical to implement educational campaigns and warning messages intended to increase users' awareness of cybersecurity risks.

Gamification, which refers to the application of game design principles in nongaming contexts, is an emerging technology that shows promise in addressing these gaps. It can be integrated with cybersecurity awareness training programs to tackle cybersecurity threats (Thakur and Kumar, 2021; Misra et al., 2017; Scholefield and Shepherd, 2019). Our study was motivated by the lack of research on the use of mobile augmented reality techniques to educate people about cybersecurity threats and raise overall cybersecurity awareness. To address this gap, we developed an AR based game, CybAR, for the Android platform. Although Augmented Reality techniques has been studied in other disciplines (Krasniqi, Berisha, and Pula, 2019), it has just started to be examined in the cybersecurity field. For the present study, the participants were shown an Augmented Reality app called CybAR that can provide useful information regarding security awareness. Key elements of the CybAR game interface were selected based on Technology Threat Avoidance Theory (TTAT) in order to enhance user interaction and to measure the effect of the game on coping appraisal factors, threat appraisal factors, avoidance motivation and risky online avoidance behaviour, as shown in Figure 1 (Liang and Xue, 2010).

This paper produces a further review of the literature applying TTAT to cybersecurity behaviour. Past TTAT studies focused more on the factors of coping and threat appraisal. Threat appraisal is identified by perceived vulnerability and susceptibility to risks, as well as rewards associated with unsafe behaviours. Coping appraisal is determined by coping response efficacy, self-efficacy and response costs associated with safe or adaptive behaviours (Arachchilage et al., 2016). Further, many studies have looked at the role of TTAT predictors on self-reported intended cybersecurity behaviour instead of attempting to access students' current cybersecurity behaviour. Therefore, the objective of this paper is to investigate the relationships between TTAT factors that influences safe cybersecurity behaviour.

In this study, data from a survey of 128 students at Macquarie University were collected and analysed. The TTAT model was used to investigate the influence of TTAT factors on cybersecurity avoidance motivation using structural equation modeling (SEM) and partial least squares (PLS) regression. The study also examined the impact of individuals' decision-making style on risky online avoidance behaviour as well as the relationship between gender and risky online avoidance behaviour. The findings help to identify users who are more susceptible to potentially dangerous security behaviours.

THEORETICAL BACKGROUND

Gamification emerged as a concept of interest in the field around 2010 (Jin et al., 2018). Several researchers have demonstrated multiple benefits from cybersecurity games such as Control-Alt-Hack, Protection Poker, CyberCIEGE, Anti-Phishing Phil and What.Hack (Wen et al., 2019). A few games

have been designed to teach cybersecurity concepts. The effectiveness of these games suggests that a mobile-based application focused on raising cybersecurity awareness would be a useful tool and justifies the development of an augmented reality (AR) game designed to increase cybersecurity awareness and knowledge in an active and entertaining way.

Augmented Reality (AR) has recently emerged as a technology that can enhance users' experience by overlaying computational information onto their reality. Azuma defined augmented reality as "an interactive experience of a real world environment where the objects that reside in the real world are enhanced by computer-generated perceptual information, sometimes across multiple sensory modalities, including visual, auditory, haptic, somatosensory and olfactory."(Azuma et al., 2001). Despite the popularity of AR applications in various fields, such as education, marketing, medicine and navigation (Alqahtani et al., 2018), no previous AR-based application has been developed to educate users about cybersecurity attacks and raise their cybersecurity awareness.

In the literature, Health Belief Model (HBM) theory (Rosenstock, 1974) and Protection Motivation Theory (PMT) (Rogers, 1975) have been used widely to explain users' intention to behave securely in a cybersecurity context, and how and when users adopt adaptive or maladaptive behaviours when they are informed of a threatening security incident. In 2009, Liang and Xue. extended the PMT by adding and refining multiple factors, and expanding/renaming the attitude change PMT outcome area to adopt different coping behaviours in TTAT (Liang and Xue, 2010). Noxiousness and probability PMT factors were combined into a new aggregate TTAT factor named perceived threat, consisted of two sub-factors: perceived susceptibility and perceived severity. The efficacy of PMT factor was also further refined as an aggregate factor called perceived avoidability, comprised of three sub-factors: a) perceived effectiveness, b) perceived cost, and c) self-efficacy of a coping response. Self-efficacy reflects confidence in one's ability to apply avoidance behaviour. Finally, TTAT coping behaviours are further refined to differentiate between emotion-focused coping to not administer an avoidance behaviour, and problem focused coping to avoid, mitigate, or nullify a threat by applying avoidance behaviour.

Our study in this paper identifies the factors that motivate individuals to continue to pursue cybersecurity avoidance behaviours beyond their avoidance motivation. We propose a theoretical model of cybersecurity avoidance behaviour that extends beyond current IS security theory. Using TTAT as a theoretical foundation, we position perceived severity, perceived susceptibility, fear, self efficacy, safeguard effectiveness and safeguard cost as significant determinants of security avoidance behaviour continuance.

Therefore, we proposed the following hypotheses:

H1. *Perceived severity positively influences students' fear and hence motivation to avoid cyber threats.*
H2. *Perceived susceptibility positively influences students' fear and hence motivation avoid cyber threats.*
H3. *Perceived susceptibility positively influences perceived severity.*

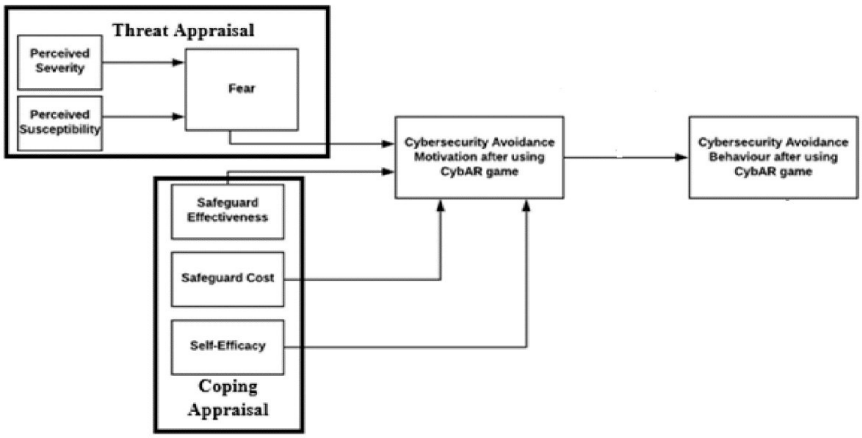

Figure 1: Research model.

H4. *Fear significantly affects students' cybersecurity avoidance motivation.*
H5. *Safeguard effectiveness positively affects students' motivation to adopt cybersecurity avoidance behaviour.*
H6. *Self-efficacy positively affects students' motivation to adopt cybersecurity avoidance behaviour.*
H7. *Self-efficacy positively affects students' cybersecurity avoidance behaviour.*
H8. *Safeguard cost negatively affects students' motivation to adopt cybersecurity avoidance behaviour.*
H9. *Students' cybersecurity avoidance motivation is positively related to their cybersecurity avoidance behaviour.*

METHODOLOGY

The constructs of TTAT have been identified in previous research as antecedents of online safety behaviour (See Figure 1). The present study examined the relationships among a number of TTAT factors (fear, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity and perceived susceptibility) as predictors of avoidance motivation. Avoidance motivation is also a predictor of avoidance behaviour. We used the word fear instead of perceived threat, as suggested by Boss et al. (2015). The research model for this study is shown in Figure 1.

SURVEY SUBJECTS AND DISTRIBUTION PROCESS

A total of 128 out of 143 students played the CybAR game and then completed an online questionnaire hosted on the Qualtrics platform without substantial missing data. The study criteria required all participants to be 18 years of age or older and have an Android tablet or Android phone. Invitations to participate were distributed to students at Macquarie University

via social media (Facebook and Twitter) and flyers posted in different locations on campus. All participants received information about the purpose of the game and the nature of the study and gave informed consent. There are some shortcomings in existing gamified approaches to education about cybersecurity challenges. Thus, our goal was to replace training programs that typically focus on reading about cybersecurity with a serious Augmented Reality game that mimics the actual forms of cybersecurity attacks. One of the main aims of CybAR was to provide more comprehensive education about cybersecurity attacks and to do so in a way that closely matches how they occur in the real world.

MEASUREMENTS

In this study, we use validated items from the prior research as constructs of the proposed model. We renamed a few concepts for reflecting the purpose of this study (refer to Table 1). We borrowed the items for each factor of TTAT model from Liang and Xue's theoretical model as presented in Table 1 (Liang and Xue, 2009). We used findings of privacy literature in information system representing the negative impact of cyberattacks to evaluate the number of items concerned with fear, perceived susceptibility and perceived severity (Smith et al., 1996). We used health behaviour research for developing safeguard effectiveness, safeguard cost and self-efficacy elements (Downs et al., 2007). The technology adoption research is used for measuring the growing number of avoidance motivation items based on behavioural intention measures by focusing on threat avoidance (Davis, 1989). Cybersecurity awareness behaviour is evaluated using six self-developed items and three items borrowed from the study (Davis, 1989). In total, there are 35 items for evaluating the eighth constructs of Liang and Xue's theoretical model (2009).

The questionnaire used in this study comprises four items concerned with fear, four items concerned with perceived severity, three items concerned with perceived susceptibility, three items concerned with safeguard effectiveness, three items concerned with safeguard cost, five items concerned with self-efficacy, four items concerned with avoidance motivation, and nine items concerned with threat avoidance behaviour. We attempt to keep these items of online questionnaire simple and easy for encouraging participants to complete the questionnaire. The responses were constructed on a 5-point Likert scale from "strongly disagree" (1) to "strongly agree" (5). All of the questionnaire items were close-ended to facilitate analysis.

ANALYSIS AND PRELIMINARY RESULTS

Two software tools were employed in data analysis. First, the survey data were recorded by Qualtrics and imported to SPSS. SPSS software is readily available and can be used to generate descriptive statistics and support the process of data analysis. Various analyses were performed using SPSS. Descriptive statistics were used to analyze each variable separately and to summarise the demographic characteristics of participants. Also, using SPSS,

Table 1. Technology threat avoidance theory items.

Constructs	Items
Perceived severity	It is extremely likely that my devices will be infected by a cybersecurity attacks in the future
	My chances of getting cybersecurity attacks are great.
	I feel cybersecurity threats will infect my computer in the future
	It is extremely likely that cybersecurity threats will infect my computer
Perceived susceptibility	Having my devices hacked by cybersecurity attacks is a serious problem for me.
	Cybersecurity attacks would steal my personal information from my computer without my knowledge.
	Cybersecurity attacks would invade my privacy.
Fear	My personal information collected by Cybersecurity attacks could subject to unauthorized secondary use.
	Cybersecurity attacks pose a threat to me
	Cybersecurity attacks is a danger to my computer
	It is dreadful to use my computer if it being attacked by cybersecurity attacks
Safeguard effectiveness	CybAR application would be useful for detecting cybersecurity attacks
	CybAR application would increase my performance in protecting my computer from cybersecurity attacks
	CybAR application would enable me to detect cybersecurity attacks on my computer faster
Safeguard cost	It will take very less time to gain awareness about cybersecurity attacks through CybAR application
	It will take less cost to gain awareness about cybersecurity attacks through CybAR application
	Using CybAR application for detecting cybersecurity attacks is convenient for me
Self-efficacy	I would be able to use CybAR application efficiently for applying cybersecurity threats prevention behaviour.
	In case of being infected by cybersecurity attacks, I can react effectively in a timely manner
	I have the necessary skills to deal with cybersecurity attacks
	I am confident of recognizing cybersecurity attacks
	I could successfully gain anti-cyber threats behaviour if someone taught me how to do it first
Avoidance motivation	I would say positive things about the CybAR application
	I intend to obtain CybAR application to avoid cybersecurity attacks
	I predict I would use CybAR application to avoid cybersecurity attacks
	I plan to use CybAR application to avoid cybersecurity attacks
Avoidance behaviour	I used CybAR application during the experiment.
	I will continue using CybAR application frequently.
	I will use CybAR application to avoid cybersecurity attacks.
	I update my anti-cyber threats knowledge frequently through CybAR application

(Continued)

Table 1. (Continued)

Constructs	Items
	CybAR app encourages me to have strong and multiple passwords for my different accounts. CybAR app promotes me to change and review my privacy/security settings on all my accounts. CybAR app induces me to keep all applications and anti-virus software on my devices up-to date. CybAR app encourages me to not open or click attachments from people whom I don't know. CybAR app promotes me to back up important files on my devices.

the cybersecurity avoidance behaviour items (shown in Table 1) were quantified by calculating the means of the numerical codes assigned by respondents to assess the effect of gender on safe online behaviour. Second, SmartPLS Version 3.0 was used for analytics.

We received far fewer responses than we had expected. Although the questionnaire link and invitation letter were shared on social networks and posted in several places around the university, and participants were asked to pass it on to their friends, only 143 questionnaires were received. After filtering, 15 of these were found to be incomplete. There was a fairly equal distribution of males (56%) and females (44%). Regarding the age groups, the largest group of respondents (39%) was aged 25–34, followed by those aged 18–24 (28%), 35–44 (22%) and 45–54 (8%). Only 3% of participants belonged to the 55+ category. Only two options for nationality were available - Australian and non-Australian. The majority (70%) reported that they were non-Australian. Most respondents were highly educated; 62% were undergraduate university students; 17% were postgraduate students; 16% were enrolled in a 2-year college degree; and 5% were high school students.

Model Validation

This section describes the assessment and testing of the proposed model using SEM. Because PLS does not provide goodness-of-fit criteria, the procedure for testing PLS was performed in two stages: assessing the reliability and validity of the measurement model; and testing the hypotheses in the structural model.

Measurement Model: The measurement model is evaluated by estimating the internal consistency reliability. The internal consistency reliability is assessed using the values for Cronbach's alpha, composite reliability and Average Variance Extracted (AVE) (Bryman, 2004). Cronbach's alpha is a measure of internal consistency that measures the correlation between items in a scale. The Cronbach's alpha for each construct had to be greater than 0.7 (Li and Ku, 2011). Composite reliability is similar to Cronbach's alpha. It measures the actual factor loadings rather than assuming that each item is equally weighted. The standardized path loading of each item should be statistically significant. In addition, the loadings should, ideally, be at least

Table 2. Construct reliability and validity.

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Cybersecurity Avoidance Motivation	0.858	0.870	0.903	0.700
Cybersecurity Avoidance Behaviour	0.927	0.928	0.939	0.632
Fear	0.880	0.895	0.925	0.805
Safeguard Cost	0.707	0.725	0.831	0.622
Safeguard Effectiveness	0.888	0.906	0.929	0.814
Perceived Severity	0.859	0.872	0.904	0.703
Perceived Susceptibility	0.760	0.788	0.844	0.577
Self-Efficacy	0.783	0.793	0.860	0.608

greater than 0.7. AVE indicates the amount of variance in a measure that is due to the hypothesized underlying latent variable. AVE for each construct has to exceed 0.5. Values greater than 0.50 are considered satisfactory. They indicate that at least 50% of the variance in the answers to the items is due to the hypothesized underlying latent variable.

All scales in our study reached a composite reliability value of at least 0.83 (ranging from 0.831 to 0.942). Thus, they exceeded the 0.70 threshold for composite reliability. In addition, the scales exhibited high internal consistency; the lowest Cronbach's alpha was 0.71, which is above the 0.70 threshold for confirmatory research. The AVE for each construct was greater than 0.5 (ranging from 0.608 to 0.814) as shown in Tables 2. Therefore, the internal consistency reliability for the constructs was confirmed.

Construct validity consists of convergent validity and discriminate validity. Convergent validity is achieved when each measurement item correlates strongly with its proposed theoretical construct. It is checked by testing the factor loadings of the outer model. The outer model loadings for approximately all items are above 0.50. Therefore, convergent validity was established (Fornell and Larcker, 1981). However, two items were excluded because they did not meet the requirements (self efficacy 4). Discriminant validity is achieved when each measurement item correlates weakly with all other proposed constructs than the one to which it is theoretically associated. The discriminant validity of the measurement model is tested using two criteria suggested by Gefen and Straub (2000): (1) item loading to construct correlations is larger than its loading on any other constructs; and (2) the square root of the AVE for each latent construct should be greater than the correlations between that construct and other constructs in the model. The lowest acceptable value is 0.50. All items showed substantially higher loading than other factors, and the square root of the AVE for each construct exceeded the correlations between that construct and the other constructs as shown in Table 3. Therefore, discriminant validity was established.

Table 3. R square.

Constructs	R^2	Result
Cybersecurity Avoidance Motivation	0.739	Substantial
Cybersecurity Avoidance Behaviour	0.645	Substantial
Fear	0.337	Weak
Perceived Severity	0.238	Weak

STRUCTURAL MODEL

In this study, we analyze the structural model using SmartPLS version 3.0. We use 9 hypotheses for analyzing the relationship between latent variables. The structural model evaluates the path of coefficient and coefficient of determination. We explain path coefficient with t-statistics computed using bootstrapping 500 samples. These tests provide a positive or negative relationship between exogenous constructs and endogenous variables in addition to the strength of the relationship. According to Lowry and Gaskin (2014), the-value of each-relationship needs to be significant at the 0.05 alpha (needing t-value of about 1.96 or greater—absolute value).This is the criteria used for supported and non-supported hypotheses.

Coefficient of determination as R2 values. R2 provides the amount of variance of dependent variables explained by the independent variables. In our analysis, the R2 coefficient of determination indicates the predictive power of the model for each dependent construct. According to Chin (1998) suggests that the R-squared values of 0.67, 0.33, and 0.19 in PLS-SEM can be considered as substantial, moderate, and weak, respectively. Therefore, our model has the ability to explain the endogenous constructs. Our research model is able to explain 33.7% of the variance in fear, 73.9% of the variance in Avoidance Motivation and around 64.5% of the variance in Avoidance Behaviour as shown in Table 3.

The SEM results revealed that most of the proposed external variables have significant effect on avoidance motivation. Of the 4 determinants of cybersecurity avoidance motivation, fear and safeguard effectiveness were supported while and self-efficacy and safeguard cost constructs was not found to be significant on cybersecurity avoidance motivation. Fear construct was influenced by perceived severity. Also, the relationship between perceived susceptibility and perceived severity was positively significant. Finally, the path between cybersecurity avoidance motivation and cybersecurity avoidance behaviour was found to be significant.

In other words, Table 4 presents the results of the hypotheses tests; with the exception of H2, H6, H8, others proposed relationships were supported. Table 4 shows the beta scores and t-values for the relationships displayed in the research model.

It is observed that perceived severity positively affects fear threat (path coefficient 0.546; $p < 0.01$) and perceived susceptibility positively affects perceived severity (path coefficient 0.487; $p < 0.01$) as per theoretical evidence concerning the hypothesized threat appraisals. It implies that hypotheses H2 and H3 should be supported. However, perceived susceptibility has no

Table 4. Path coefficient of the research hypotheses.

Hypothesis	Relationship	Path Coefficient	T Value	P Values	Decision
H1	Perceived Severity -> Fear	0.546	3.454	0.001	Supported **
H2	Perceived Susceptibility -> Fear	0.066	0.403	0.687	Not Supported
H3	Perceived Susceptibility -> Perceived Severity	0.487	3.714	0.000	Supported **
H4	Fear -> Cybersecurity Avoidance Motivation	-0.384	3.449	0.001	Supported **
H5	Safeguard Effectiveness -> Cybersecurity Avoidance Motivation	0.951	8.000	0.000	Supported **
H6	Self-Efficacy -> Cybersecurity Avoidance Motivation	0.131	1.365	0.173	Not Supported
H7	Self-Efficacy -> Cybersecurity Avoidance Behaviour	0.562	8.085	0.000	Supported **
H8	Safeguard Cost -> Cybersecurity Avoidance Motivation	0.132	0.982	0.327	Not Supported
H9	Cybersecurity Avoidance Motivation -> Cybersecurity Avoidance Behaviour	0.316	3.973	0.000	Supported **

*Significant at P**= < 0.01, p* <0.05.

significant effect on fear of threat factor, and Table 4 shows that H2 is not supported.

The result obtained indicates that there is no significance of fear in the role of perceived susceptibility in context to participants' fear (threat). In contrast, perceived severity plays an essential role in this context. Furthermore, it can also be noticed that fear (threat) negatively affects cybersecurity avoidance motivation (path coefficient -0.384; $p < 0.01$). This implies H4 is supported.

With respect to the hypothesized coping appraisals, neither self-efficacy nor safeguard cost affects cybersecurity avoidance motivation, on the contrary to what we theorized. Thus, H6 and H8 were "not supported". However, safeguard effectiveness ($b = 0.951$; $p < 0.01$) affects cybersecurity avoidance motivation as expected. Therefore, H5 was supported. Also, as theorized, self-efficacy ($b = 0.562$; $p < 0.01$) affects cybersecurity avoidance behaviour directly without mediation. Therefore, H7 was supported. Finally, for the hypothesized effects of cybersecurity avoidance motivation on the cybersecurity avoidance behaviour in TTAT variables, the relationship is positively correlated ($b = 0.316$; $p < 0.01$). Overall, all supported hypotheses were strongly supported (H1: 0.55; H3: 0.49; H4: -0.39; H5: 0.95; H7: 0.56; H9: 0.32), and were significant at the $p < 0.01$ level.

Overall, participants' threat and coping appraisals in this study are related to more protective cybersecurity behaviours. The results of this study validate that the TTAT is a valuable conceptual framework for understanding students' cybersecurity behaviours.

DISCUSSION

This study proposed a model for evaluating individual cybersecurity behaviour via participants' self-reported protective actions. The model used the TTAT framework to analyse the various factors affecting students' behaviour based on their appraisal of cybersecurity threats and the effectiveness of coping strategies, as described in Figure 1. We used a survey-based approach, which has been widely deployed in recent relevant research (D'Arcy and Greene, 2014; Dwivedi et al., 2015; Herath and Rao, 2009; Ng and Xu, 2007). We collected data from a sample of 128 students to evaluate the conceptual model. The results indicate that the proposed TTAT model is a robust framework for investigating the role of the various factors that affect the cybersecurity behaviour of students. The results also support the hypotheses proposed in this study. Thus, it can be concluded that the proposed TTAT model is useful for evaluating the cybersecurity behaviour of individuals.

The results further showed that perceived susceptibility has a significant impact on the perceived severity of the threat. There was a strong correlation between threat susceptibility and threat severity. However, perceived susceptibility had no significant impact on students' fear threat. This implies that susceptibility does not increase one's fear to avoid risky cybersecurity behaviour. There was no significant effect of fear appraisal factors or susceptibility variables on fear of the threat, which was unexpected in the context of cybersecurity avoidance motivation. This finding is inconsistent with the TTAT model, but consistent with other IS security domains. For instance, despite Workman et al.'s (2008) findings on the significance of susceptibility in explaining the likelihood of employees omitting IS security precautions, the size of the path coefficients demonstrating such effects were too small to be considered meaningful. It seems that our respondents generally did not believe that they would face such information security threats if they did not practise safe online behaviour.

It was also observed that the severity of the threat had a positive impact on students' fear to motivate avoidance cybersecurity behaviour, which is consistent with the TTAT model and with previous empirical tests of the theory. Herath and Rao (2009), for instance, reported a similarly strong relationship between perceived severity and safe cybersecurity behaviour. Other studies, however, have reported contradictory results (Hanus and Wu, 2016; Herath and Rao, 2009). We concluded that there is a positive association between threat severity and fear experienced due to perceptions of cybersecurity threats. However, fear does not translate into positive motivation to protect oneself from cybersecurity attacks. This indicates a negative association between fear and protection motivation and is consistent with previous findings (Tsai et al., 2016; Warkentin et al., 2016). However, such an association was not considered in the hypotheses proposed in this study. It is

noted that fear arises from an appraisal of threatening stimuli as an emotional response. It engenders a cognitive and physiological reaction (Bagozzi and Gopinath, 1999). Boss et al. (2015) reported similar results using direct fear-appeal manipulations.

In the context of coping appraisal, we conclude that self-efficacy and safeguard effectiveness are significant determinants of protective cybersecurity behaviour, which is consistent with the theoretical framework (and provides support for H5 and H7). The results indicate the significance of cognitive processes in security protection. Self-efficacy and safeguard effectiveness were also identified as essential predictors of protective behaviour, which is consistent with previous research findings (Hanus and Wu, 2016; Tsai et al., 2016; Warkentin et al., , 2016).

In our study, safeguard cost had no significant impact on protective cybersecurity behaviour. This result is similar to those in some earlier studies (Hanus and Wu, 2016) but is inconsistent with the TTAT model and with other previous research (Tsai et al., 2016). However, no experimental research has been conducted in the area of information systems. This suggests that the protective features that are provided by cybersecurity companies at little or no cost are acceptable to the public. For instance, Firewall and backup data solutions are provided as inbuilt features of the operating system. Antivirus and anti-spyware software is also available free of charge, or else the cost is included in the price of new hardware

In this study, coping appraisal had a significant role in increasing cybersecurity protection motivation and behaviour in comparison to threat appraisal. This finding is in line with previous research (Hanus and Wu, 2016; Tsai et al., 2016). This observation suggests that it is more effective to inform users how to effectively avoid a potential cyber-attack rather than to threaten them with the consequences of unsafe behaviour.

LIMITATIONS AND FUTURE WORK

Several limitations of this research should be noted. First, the study employed a cross-sectional research design. Longitudinal data will enhance our understanding of what constructs affect individuals' avoidance behaviour after using the CybAR app. Second, only quantitative data were collected. Qualitative data generated from interviews or focus groups could yield insight into other factors that affect individuals' avoidance behaviour and avoidance motivation.Third, interpretation of the results was limited by the small sample size (128). A larger sample would have improved the ability to generalise the findings to a wider population. It should be noted, however, that the use of SmartPLS as a data analysis tool overcomes this limitation since it can generalise results with a very small sample size. Fourth, the study was conducted in one university so the results may not be applicable to all Australian universities, even if the education system and culture are the same.

This study integrates the concepts drawn from previous online safety research using the extended TTAT model, thus opening up many possibilities for future research in the field. For instance, the work can be expanded to consider the role of culture, security culture, education level, the Big Five

personality traits, risk-taking preferences, and total variance in cybersecurity avoidance behaviour.

This study also evaluated the prediction of individuals' security behaviour based on existing variables. The extended TTAT model we have proposed can be further explored by including coping and threat appraisal variables into the TTAT model. Specifically, safety habits and personal responsibility can be considered as strong predictors of cybersecurity motivation.

CONCLUSION

In this paper, we used a cross-sectional survey of 128 students at Macquarie University to investigate the influence of TTAT constructs on students' cybersecurity behaviour, thus extending the limited work on online safety. We found that coping appraisals (self-efficacy and safeguard effectiveness) were more important predictors of cybersecurity avoidance motivation and behaviour than threat appraisal. In contradiction to the assumptions of TTAT, the fear construct was a negative predictor in the regression analysis (r = -.384, p < .01). We observed positive correlations between threat severity and fear (r = .546, p < .01), coping self-efficacy and cybersecurity avoidance behaviour (r = .562, p < .01), and safeguard effectiveness and cybersecurity avoidance motivation (r = .951, p < .01). No relationship was observed between perceived susceptibility and fear (r = .066, p > .05) and safeguard cost and cybersecurity avoidance motivation (r = .132, p >.05).

REFERENCES

Alqahtani, H., Kavakli, M., and Sheikh, N. U. (2018). Analysis of the Technology Acceptance Theoretical Model in Examining Users' Behavioural Intention to Use an Augmented Reality App (IMAP-Campus). International Journal of Engineering and Management Research (IJEMR), 8(5), 37–49.

Arachchilage, N. A. G., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Azuma, R., Baillot, Y., Behringer, R., Feiner, S., Julier, S., and MacIntyre, B. (2001). Recent advances in augmented reality. IEEE Computer Graphics and Applications, 21(6), 34–47. https://doi.org/10.1109/38.963459

Bagozzi, R., and Gopinath, M. (1999). The Role of Emotions in Marketing Drivers of public responses toward Coronavirus outbreak and implications of social dynamics View project. Article in Journal of the Academy of Marketing Science, 27(2), 184–206. https://doi.org/10.1177/0092070399272005

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly: Management Information Systems, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bryman, A. (2004). Quantitative Data Analysis with SPSS 12 and 13. Quantitative Data Analysis with SPSS 12 and 13. https://doi.org/10.4324/9780203498187

Chin, W. W. (1998). Issues and opinion on structural equation modeling. MIS Quarterly: Management Information Systems.

D'Arcy, J., and Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. In Information Management and Computer Security (Vol. 22, pp. 474–489). Emerald Group Publishing Ltd. https://doi.org/10.1108/IMCS-08-2013-0057

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly: Management Information Systems, 13(3), 319–339. https://doi.org/10.2307/249008

Downs, J. S., Holbrook, M., and Cranor, L. F. (2007). Behavioral response to phishing risk. In ACM International Conference Proceeding Series (Vol. 269, pp. 37–44). https://doi.org/10.1145/1299015.1299019

Dwivedi, Y. K., Kapoor, K. K., and Chen, H. (2015). Social media marketing and advertising. The Marketing Review, 15(3), 289–309. https://doi.org/10.1362/146934715x14441363377999

Filkins, B. (2016). IT Security Spending Trends. SANS Institute InfoSec Reading Room, 36.

Fornell, C., and Larcker, D. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), 39–50. https://doi.org/10.1177/002224378101800104

Gefen, D., Straub, D., and Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems, 4. https://doi.org/10.17705/1cais.00407

Hanus, B., and Wu, Y. "Andy." (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

Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Howard, D., and Prince, K. (2011). Security 2020: Reduce Security Risks This Decade. Wiley 223 Publishing.

Jin, G., Tu, M., Kim, T. H., Heffron, J., and White, J. (2018). Game based cybersecurity training for High School Students. In SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education (Vol. 2018–January, pp. 68–73). Association for Computing Machinery, Inc. https://doi.org/10.1145/3159450.3159591

Krasniqi, B. A., Berisha, G., and Pula, J. S. (2019). Does decision-making style predict managers' entrepreneurial intentions? Journal of Global Entrepreneurship Research, 9(1), 1–15. https://doi.org/10.1186/s40497-019-0200-4

Li, C. Y., and Ku, Y. C. (2011). The effects of persuasive messages on system acceptance. In PACIS 2011 - 15th Pacific Asia Conference on Information Systems: Quality Research in Pacific. Retrieved from http://aisel.aisnet.org/pacis2011/110

Liang, H., and Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly: Management Information Systems, 33(1), 71–90. https://doi.org/10.2307/20650279

Liang, H., and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394–413. https://doi.org/10.17705/1jais.00232

Liang, H., and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394–413. https://doi.org/10.17705/1jais.00232

Misra, G., Arachchilage, N. A. G., and Berkovsky, S. (2017). Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. Arxiv.Org. Retrieved from https://arxiv.org/abs/1710.06064

Ng, B. Y., and Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. In PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises. Retrieved from https://www.researchgate.net/publication/221229127

Ng, B. Y., Kankanhalli, A., and Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosenstock, I. M. (1974). Historical Origins of the Health Belief Model. Health Education and Behavior, 2(4), 328–335. https://doi.org/10.1177/109019817400200403

Scholefield, S., and Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 11594 LNCS, pp. 191– 203). Springer Verlag. https://doi.org/10.1007/978-3-030-22351-9_13

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly: Management Information Systems, 20(2), 167–195. https://doi.org/10.2307/249477

Thakur, K., and Kumar, G. (2021). Nature Inspired Techniques and Applications in Intrusion Detection Systems: Recent Progress and Updated Perspective. Archives of Computational Methods in Engineering, 28(4), 2897–2919.

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

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. Decision Support Systems, 92, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Wen, Z. A., Lin, Z., Chen, R., and Andersen, E. (2019). What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. In Conference on HumanFactors in Computing Systems - Proceedings. https://doi.org/10.1145/3290605.3300338

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005