BEFORE-AFTER INVESTIGATION ON BANK INFORMATION SECURITY DRILL: SEVERITY, SUSCEPTIBILITY AND FEAR

Cai Zhi Meng, Anyang Normal University, Management and Science University

Siti Khalidah Mohd Yusoff, Management and Science University

Brian Sheng-Xian Teo*, Management and Science University

ABSTRACT

The application of various APPS leads to threats to bank information security, so there is an urgent need for an effective method to improve the information security awareness of bank employees. The purpose of this before-after investigation is to emphasize the importance of information security drill by comparing the same factors affecting bank Employees' information security awareness based on extended parallel processing model (EPPM). Drawing on a before-after research design, this article examines the links of perceived severity, fear, perceived susceptibility, self-efficiency, response efficacy and bank employees' information security awareness. Research results indicate that experience with infection of malwares can enhance bank employees' defensive behavior, which proves information security drill is useful for information security education among bank employees. In the before-test, the relationships between perceived severity and response efficacy, perceived susceptibility and response efficacy, perceived severity and self-efficacy, fear and awareness are not significant. But in the after-test, not only all relationships are supported, but also all the t-values have increased. It indicate that information security drill can improve the risk-resisting ability and the banks can combine information security drill with vocational education, knowledge popularization, staff training, daily demonstration and advertising to reduce the financial and competing cost related with financial fraud and hacker attacks. It proves that drill can test the bank's existing information security rules, improve the tacit understanding of various departments, and achieve the best results with less consumption.

Keywords: Extended Parallel Processing Model, Before-after Test, Information Security Drill, Information Security Awareness, Information Security Training

INTRODUCTION

One of the more critical aspects in financial industry is to ensure that the bank employees can understand the importance of protecting financial privacy when more mobile devices are applied in their daily financial work. More and more APPs for work, entertainment, finance, shopping, social interaction, learning, music production, etc. have become a part of many people's lives. Those APPs from the third parties have been installed in phones, tablets and personal computers, which may provide opportunities for all kinds of malware to steal users' financial privacy. Although most bank employees have showed their concerns about the violation of financial privacy, the careless behavior or lack of awareness of financial privacy prevention often lead to the theft of financial privacy on mobile devices (Barth, 2019). Thus, the acts on financial privacy protection have become a popular research focus especially in financial privacy protection aspect since more and more financial frauds come into stage in recent years. Studies about financial privacy protection are carried out enormously in varieties of fields, including development of information software, hardware encryption and artificial intelligence recognition technology (Chen, 2019; Hajek, 2017; Zhi, 2019; Joon, 2019). However, in spite of

Citation Information: Meng, C.Z., Yusoff, S.K.M., & Xian, B.S. (2021). Before-after investigation on bank information security drill: Severity, susceptibility and fear. *Journal of Management Information and Decision Sciences, 24*(S6), 1-13.

all these efforts, methods or technologies' development will be no use unless the bank employees' information security awareness's development is well implemented. Information security drills are the rehearsal activities of bank employees to perform their respective responsibilities and tasks when actual emergencies occur under the conditions of pre-virtual events. Simply, it is a coping exercise that simulates the occurrence of emergencies. Previous researches have proved that drills can effectively reduce casualties and property losses when emergencies occur, and quickly restore normal conditions from various disasters (Rahouti, 2020; Steve, 2020). This research is designed to compare the results of before-after information security drills in order to find what factors will improve bank employees' information security awareness (ISA here-after). Plenty of previous researches have applied comparative method to different research fields, including international education, individual and institutional competitiveness, cultural difference and business strategy (Spiteri, 2018; Hamilton, 2017; Gromada, 2019; Warwick, 2013). Before-after test method is also applied to this research because a before-after evaluation can repeat the experiment under the same conditions and observe the degree of its influence on the experimental results, and by this way, we can avoid the accidental results, draw accurate and scientific conclusions. The before-after test is widely used in the field of scientific researches, such as road safety and traffic problems (Elvik, 2017; Zheng, 2019). Therefore, the purpose of this before-after investigation is to emphasize the importance of information security drill by comparing the same factors affecting bank Employees' information security awareness based on extended parallel processing model (EPPM here-after). In this regard, it is intended to measure how perceived severity, fear, perceived susceptibility, self-efficiency and response efficacy's role in bank employees' information security awareness.

LITERATURE REVIEW

Varieties of previous researches and approaches have been applied into the field of protecting financial privacy and crisis management. Quite a lot of measures have been applied to information security protection. For example, banks reduce dependence on other's technology and try to use their own software and hardware products as much as possible. Banks try to improve the security verification of the two important links of login and payment. Additionally, banks introduce electronic authentication technology and other measures to improve the information security of data during transmission. However, establishing a complete internal crisis management system to improve the risk awareness is more important than hardware capability improvement. Extensive previous researches prove that enhancing employees' crisis management ability is an effective way to deal with emergencies (Melissa, 2017; Kubiak, 2019; Waele, 2020). Therefore, enhancing the professional quality of employees has reached consensus in various industries (Miller, 2005; Lucio, 2005; Lefebvre, 2009 Han, 2011; Kramera, 2018). At the technical level, some previous researches develop methods by integrating diverse data to look for fraud information in financial statement or announcement of listed companies (Chen, 2019), whereas some other previous researches focus on financial institutions' internal fraud detection by measuring the probability of fraud (Joon, 2019). Based on rapid development of artificial intelligence technology, more and more researchers have applied face recognition and data mining technology in protecting financial privacy (Hajek, 2017). Barth, et al., (2019) prove that knowledge and other related factors are positively affected on mobile devices users' online privacy behavior. As financial technology has become more popular in financial industry and social network is connecting everything from small communities to global ones (Jia, 2019), new Privacy security agreement protocols are proposed to filter out applet malware to prevent mobile devices from being infected by malware (Li, 2019). Since most of the bank employees are high performers, concerns of loss of financial privacy may lead to overload pressure, which in turn bring job dissatisfaction to them. Based on above discussion, only limited existing literatures have given detailed investigation on how to improve bank employees' information security awareness by drill. Specially, it remains blanket in research of comparing the before and after test results to investigate bank employees' crisis management ability in drill.

Extended Parallel Processing Model (EPPM) and Hypotheses

According to Protection Motivation Theory （PMT）, the relationship between fear and action is not linear. PMT believes that when people take protective actions, there are also two sets of considerations, which are called threat appraisal and coping appraisal (Redmond, 2015). In the threat assessment, people will consider two specific questions: How severe is the threat (perceived threat severity)? How likely is I to suffer such a threat (perceived threat vulnerability)? In response assessments, people will consider two other specific questions: how effective is the solution recommended to me (perceived response efficacy)? Do I have the ability to act according to recommendations (perceived self-efficacy)?

Like PMT, the extended parallel process model (EPPM) also agrees that when faced with information about fear, people will pay attention to threat assessment and response assessment. However, EPPM has taken another step forward. It believes that the appeal of fear will also activate the other two parallel psychological processes. On the one hand, people may want to control the threat brought by fear, that is, threat control processes; on the other hand, people may want to control their perception of threats, that is, fear control processes. The two key conclusions of EPPM are: when the perceived threat is high and the effectiveness perception is high, the threat control process will be activated; when the perceived threat is high and the effectiveness perception is low, the fear control process will be activated. Extended Parallel Processing Model was designed to predict how individuals react to make multiple appraisals in a fear appeal situation. The first appraisal of EPPM is about the relative threat of a message, indicating that if messages are deemed to be threatening, individuals may then make a secondary appraisal. Thus, in secondary appraisal, individuals assess their ability to manage the presented threat.

EPPM theory is one of the most popular theories in explaining perception of efficacy and threat as key concepts to suggest the perception of efficacy and threat to affect results by interacting. Threat aspect consists of severity and susceptibility, whereas efficacy aspect consists of self-efficiency and response effectiveness. Specially, although logic behind the relations indicates that the critical point may occur at a proper time during exposure to some specific situations, the predictions or explanations about the same constructs may vary according to different people or events.

When bank employees perceive high threats, it means that bank employees are aware of the serious harm caused by information security. When their efficiency perception is high, it means that bank employees really think they have the ability to prevent information security disasters. At this time, they often make attempts to prevent disasters, that is, threat control. However, if the perceived threat is high and the effectiveness perception is low, although bank employees are aware of the serious harm caused by information security disasters, they do not consider themselves capable of controlling disasters. They will feel fear and despair. EPPM's inspiration to us is that information security training for bank employees should not only bring fear to them, but need to tell them that information security training is useful, and you can be trained to deal with and prevent information security risks in the future. Figure 1 shows the detailed construct information of EPPM theory. According to Protection Motivation Theory (PMT), the relationship between fear and action is not linear. PMT believes that when people take protective actions, there are also two sets of considerations, which are called threat appraisal and coping appraisal (Redmond, 2015). In the threat assessment, people will consider two specific questions: How severe is the threat (perceived threat severity)? How likely is I to suffer such a threat (perceived threat vulnerability)? In response assessments, people will consider two other specific questions: how effective is the solution recommended to me (perceived response efficacy)? Do I have the ability to act according to recommendations (perceived self-efficacy)?

Like PMT, the extended parallel process model (EPPM) also agrees that when faced with information about fear, people will pay attention to threat assessment and response assessment. However, EPPM has taken another step forward. It believes that the appeal of fear will also activate the other two parallel psychological processes. On the one hand, people may want to control the threat brought by fear, that is, threat control processes; on the other hand, people may want to control their perception of threats, that is, fear control processes. The two key conclusions of EPPM are: when the perceived threat is high and the effectiveness perception is high, the threat control process will be activated; when the perceived threat is high and the effectiveness perception is low, the fear control process will be activated. Extended Parallel Processing Model was designed to predict how individuals react to make multiple appraisals in a fear appeal situation. The first appraisal of EPPM is about the relative threat of a message, indicating that if messages are deemed to be threatening, individuals may then make a secondary appraisal. Thus, in secondary appraisal, individuals assess their ability to manage the presented threat.

EPPM theory is one of the most popular theories in explaining perception of efficacy and threat as key concepts to suggest the perception of efficacy and threat to affect results by interacting. Threat aspect consists of severity and susceptibility, whereas efficacy aspect consists of self-efficiency and response effectiveness. Specially, although logic behind the relations indicates that the critical point may occur at a proper time during exposure to some specific situations, the predictions or explanations about the same constructs may vary according to different people or events.

When bank employees perceive high threats, it means that bank employees are aware of the serious harm caused by information security. When their efficiency perception is high, it means that bank employees really think they have the ability to prevent information security disasters. At this time, they often make attempts to prevent disasters, that is, threat control. However, if the perceived threat is high and the effectiveness perception is low, although bank employees are aware of the serious harm caused by information security disasters, they do not consider themselves capable of controlling disasters. They will feel fear and despair. EPPM's inspiration to us is that information security training for bank employees should not only bring fear to them, but need to tell them that information security training is useful, and you can be trained to deal with and prevent information security risks in the future. Figure 1 shows the detailed construct information of EPPM theory.

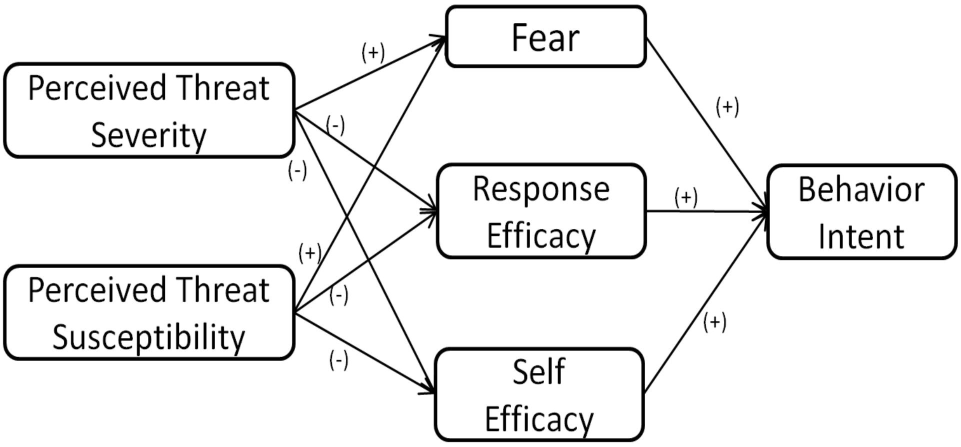


FIGURE 1
EXTENDED PARALLEL PROCESSING MODEL

EPPM theory has already been applied into variety of research field. Drawing on EPPM theory, Shi & Smith (2015) prove that repeated exposure to certain fear appeal messages may lead to high infection probability. Redmond, et al., (2015) indicate that EPPM theory can help to why education and counseling are necessary for pregnancy healthcare. EPPM theory has been applied in varieties of research fields such as hearing protection (Kotowski, 2011; Smith, 2008), HIV prevention (Murray, 2001) teen pregnancy (Witte, 1997) and alcohol usage reduction (Moscato, 2001; Wolburg, 2001; Zisserson, 2007). In this research, the EPPM theory is adapted to environment of bank employees' financial privacy protection awareness. EPPM indicates that the combination of perceived efficacy and perceived risk can lead to risk reduction behavior, whereas fears without positive efficacy instructions can cause maladaptive fear control instead of protective danger control. Therefore, EPPM is useful in financial data protection campaigns when theft of financial data poses a real or perceived threat to the whole financial systems. Safety training or education for financial practitioners using EMMP theory may offer actionable and realistic instructions about how to deal with risk and help bank employees develop useful and realistic solutions because quite a few of the bank employees have no idea about how to prevent malware attack in daily works and can't estimate the possible serious consequences. Thus, financial privacy protection awareness is such an important research objective among financial practitioners that it is necessary to summarize the EPPM characteristics to investigate how financial practitioners' behavioral change in a before-after test. Through a thorough analysis of EMMP for information security awareness (ISA), the optimized research model is shown in figure 2.

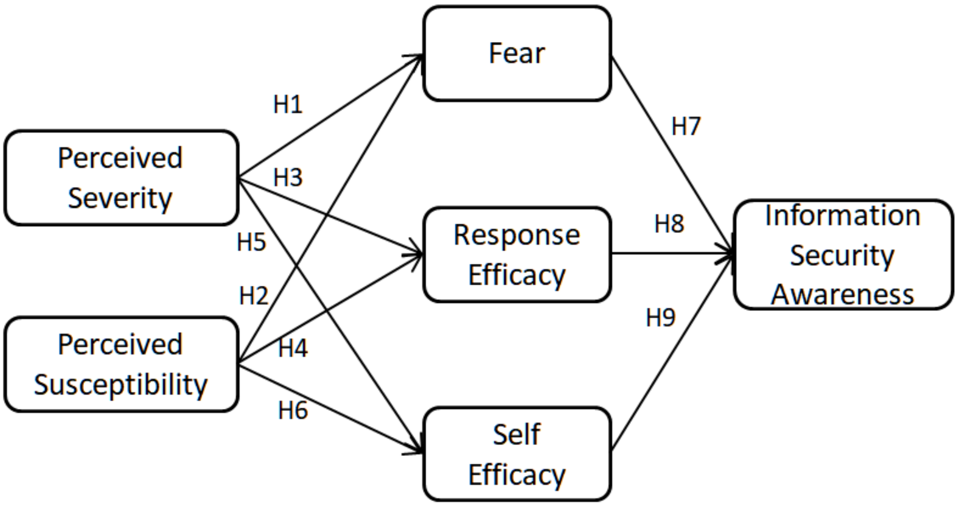


FIGURE 2
RESEARCH MODEL

Since most of the constructs of EPPM remain in the optimized research model, the hypotheses are thus as follows.

In EPPM theory, perceived severity indicates beliefs related to the consequences of a particular event (Roberto, 2000) or to the importance or severity of the threat (Witte, 1998; Witte, 1996). It indicates the idea that bank employees hold toward to the importance or significance of the theft of financial data. When the bank employees' perception of severity of theft of financial data increases, they may feel helpless in dealing with current dilemmas, and then they feel more fear. It will be a burden to financial practitioners. Specially, variations in perceived of information security threats could cause financial practitioners reassess the reaction to protect their financial data and make them become less efficient in response to malware and fight against malware with less self-efficacy. Therefore:

H1: Perceived severity positively affects fear.
H3: Perceived severity negatively affects response efficacy.
H5: Perceived severity negatively affects self-efficacy.

Perceived susceptibility refers to the belief in the risk of being threatened (Witte, 1998; Witte, 1996). Similar to perceived severity, perceived susceptibility indicates financial practitioners' probability to encounter the malware. As financial practitioners' perception of

Citation Information: Meng, C.Z., Yusoff, S.K.M., & Xian, B.S. (2021). Before-after investigation on bank information security drill: Severity, susceptibility and fear. *Journal of Management Information and Decision Sciences, 24*(S6), 1-13.

susceptibility increases and malware may become a burden to bank employees, they fear more in dealing with malware, and then, they may feel helpless to protect their financial data, become less efficient in response to malware and hardly find solutions to fight against it with self-efficacy. Therefore:

H2: Perceived susceptibility positively affects fear.

H4: Perceived susceptibility negatively affects response efficacy.

H6: Perceived susceptibility negatively affects self-efficacy.

Fear represents an internal negative emotional response, including the psychological and physical aspects caused by serious experience about threats (Witte, 1998; Witte, 1996). Fear has been proved in different previous researches about the positive or negative relationships with behaviors (Lorenc, 2012; Omer, 2018; Shin, 2017). The fear that financial practitioners perceive in dealing with malware may include different items, such as fear of economic loss, social level loss, performance failure and privacy loss. In order to conquer the fear, the bank employees may decide to learn more technics, reading more rules and seek useful tools to be more awareness in dealing with malware. Therefore:

H7: Fear positively affects ISA.

Self-efficacy indicates people's belief in their ability to respond to recommendations to avoid threats (Gore, 2005). Response efficacy represents a belief in the effectiveness of the proposed response in preventing or avoiding threats (McMahan, 1998; Roberto, 2000). Plenty of previous studies have proved the relationship between self-efficacy, response efficacy and behaviors in different fields including road safety (Tay, 2001), cyber security (Lawson, 2016) and health examination (Huang, 2016). Although some bank employees know how to use tools, software, rules and strategies in dealing with malware, they could probably feel confused or apprehensive about their own ability in using them due to the lack of high response efficacy and self-efficacy. Those who are self-efficacy and responsive may show a more positive view and are eager to seek more benefits to increase awareness of malware. Therefore:

H8: Response efficacy positively affects ISA.

H9: Self efficacy positively affects ISA.

METHOD OF RESEARCH

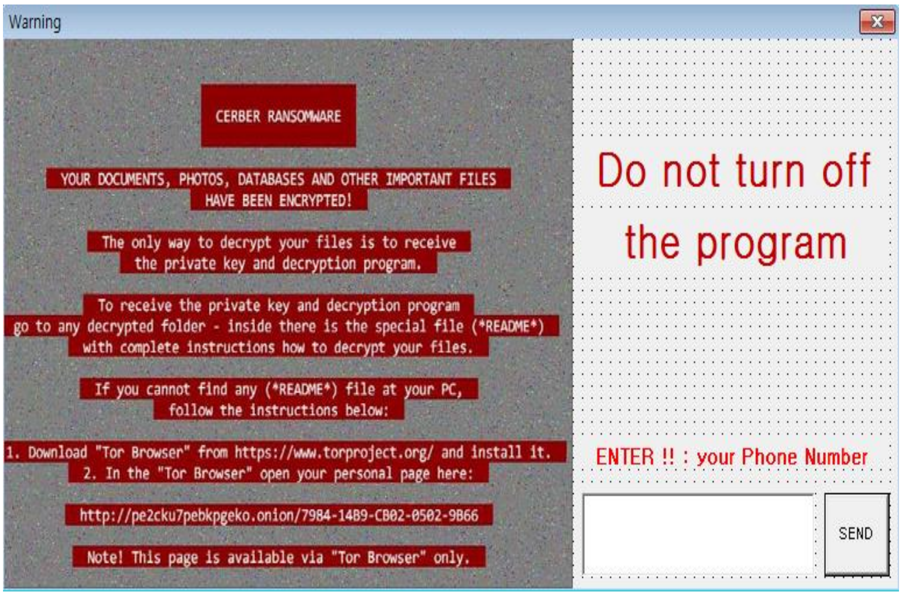
This study aims to conduct empirical studies to ensure that bank employees' ability to perceive and respond to malware threats is an effective way to protect their financial information. The research was conducted on 163 bank employees who are in private banking department or personal financial business department, which means they visit customers frequently and deal with a lot of financial information every day in their own notebooks, tablets and desktops. In addition, the subjects of the experiment are to recruit and conduct applications to obtain clear data.

All the bank employees were volunteered for this experiment, and all laptops were provided by researchers. All bank employees who join the training courses should agree to a disclaimer, which is 1) I volunteered to attend the training course and fill in an anonymous questionnaire. 2) I openly and voluntarily accept information security drill in the training course. 3) All information is authorized to be disclosed. 4) There is no conflict of any interest. The training course and drill is approved by the relevant authorities.

At first, they received three hours of information security training, and then were given a questionnaire about the adoption of financial security awareness to fill in. Secondly, they were asked to take a test about financial knowledge in one hour. They were told that the top twenty with the highest score can be rewarded our movie coupons. Thirdly, when they finished the test and click to submit, a window appeared to tell them that the laptops had been infected with a malware and all files had been encrypted. Fourthly, when they felt surprised by what had happened, the researchers came over to calm them down and told them this was part of the information security drill. Finally, they were invited to fill in the same questionnaire again. Anyway, all participants received four movie coupons as reward. This design is intent to verify

Citation Information: Meng, C.Z., Yusoff, S.K.M., & Xian, B.S. (2021). Before-after investigation on bank information security drill: Severity, susceptibility and fear. *Journal of Management Information and Decision Sciences, 24*(S6), 1-13.

the difference about how bank employees' awareness after a real experience of financial security threatening. Figure 3 shows the warning information window (infectious warning window).



Warning

CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*README*)
with complete instructions how to decrypt your files.

If you cannot find any (*README*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://pe2cku7pebkpgeko.onion/7984-14B9-CB02-0502-9B66

Note! This page is available via "Tor Browser" only.

Do not turn off the program

ENTER !! : your Phone Number

FIGURE 3
VIRTUAL MALWARE PROGRAM (INFECTIOUS WARNING WINDOW)

Measurement and Data analysis

The perceived severity factor is measured by three items. ("I believe that loss of financial privacy is extremely harmful." "I believe that loss of financial privacy has serious negative consequences." "I believe that loss of financial privacy is severe."). We use 7-likert scale to test the items. 1 means strongly disagreement and 7 means strongly agreement.

The perceived susceptibility construct is measured by three items. ("I am at risk of loss of financial privacy." "It is possible that I will get loss of financial privacy" "It is likely that I will get loss of financial privacy"). We use 7-likert scale to test the items. 1 means strongly disagreement and 7 means strongly agreement.

The fear construct is measured by three items. ("In my opinion, loss of financial privacy is very dangerous." "The consequences of loss of financial privacy are serious." "Loss of financial privacy will ruin my career and reputation"). We use 7-likert scale to test the items. 1 means strongly disagreement and 7 means strongly agreement.

The self-efficacy construct is measured by three items. ("I have the time to find ways to stop loss of financial privacy." "I can easily find ways to avert loss of financial privacy." "I am able to find ways to prevent loss of financial privacy"). We use 7-likert scale to test the items. 1 means strongly disagreement and 7 means strongly agreement.

The response efficacy construct is measured by three items. ("Learning privacy protection skills is an effective way to protect myself from loss of financial privacy." "Learning privacy protection skills works to protect myself from loss of financial privacy." "Complying with related financial privacy protection rules is an effective way to avoid loss of financial privacy."). We use 7-likert scale to test the items. 1 means strongly disagreement and 7 means strongly agreement.

The information security awareness construct is measured by three items. ("I plan to take good care of financial privacy in my financial work." "I intend to tell other people about the importance of protecting financial privacy." "I would like to participate in financial privacy prevention training."). We use 7-likert scale to test the items. 1 means strongly disagreement and 7 means strongly agreement.

Descriptive statistics

Of these 163 participants, 106 were men (65.0%) and 57 were women (35.0%). The majority of respondents were aged between 30 and 40 (42.3%). Table 1 shows the respondents of demographics. It is necessary to compare the constructs of before/after tests' mean and standard deviation to find out the gaps between the same construct, because the gap shows the different responses to the same questionnaire in before/after tests. Table 2 shows the comparison of before/after mean and standard deviation.

Table 1
DEMOGRAPHIC ANALYSIS

Category	Subject	N	%
Gender	Male	106	65.0%
	Female	57	35.0%
Education Level	High School	0	0%
	Bachelor	98	60.1%
	Master	53	32.5%
	PHD	12	7.4%
Age	23-30	52	31.9%
	30-40	69	42.3%
	40-50	23	13.6%
	More than 50	19	12.2%
Term of Financial Working Experience	Less Than3 years	31	19.0%
	3-6years	87	53.4%
	6-9 years	35	21.5%
	More than 9 years	10	6.1%

Table 2
COMPARISON OF BEFORE/AFTER MEAN & STANDARD DEVIATION

Construct	Before		After		Gap
	Mean	SD	Mean	SD	
Perceived Severity	4.204	1.260	5.387	1.160	1.183
Perceived Susceptibility	3.983	1.183	4.885	1.244	0.902
Fear	5.212	1.387	5.674	1.050	0.462
Self-efficiency	3.610	1.460	3.862	1.540	0.252
Response Efficacy	3.608	1.235	4.724	1.355	1.116
ISA	4.605	1.464	5.330	1.160	0.725

Measurement Model and Results

Table 3 lists the alpha values for Cronbach, all of which exceed the recommended threshold of 0.7 to demonstrate its reliability. The composite reliability is also higher than the recommended threshold of 0.7 to prove its convergence (Sun, 2019). AVE is higher than the recommended threshold of 0.5 to prove its convergence effectiveness (Sun, 2020). The before-test results are in bracket whereas the after-test results are without blanket.

Table 3
CONVERGENT VALIDITY, COMPOSITE RELIABILITIES TESTING RESULTS

Construct	Item	Standardized Loading	Composite Reliability (CR)	AVE
Perceived Severity (PS)	PS1	0.813(0.794)	0.952 (0.912)	0.809 (0.785)
	PS2	0.920(0.841)		
	PS3	0.808(0.751)		
Perceived	PSU1	0.973(0.902)	0.937	0.817

Susceptibility (PSU)	PSU2	0.818(0.783)	(0.895)	(0.767)
	PSU3	0.904(0.862)		
Fear (FE)	FE1	0.909(0.814)	0.958 (0.916)	0.931 (0.908)
	FE2	0.913(0.827)		
	FE3	0.975(0.958)		
Self-efficiency (SE)	SE1	0.919(0.909)	0.919 (0.883)	0.911 (0.855)
	SE2	0.926(0.858)		
	SE3	0.964(0.923)		
Response Efficacy (RE)	RE1	0.898(0.847)	0.941 (0.907)	0.803 (0.774)
	RE2	0.939(0.836)		
	RE3	0.891(0.803)		
ISA (ISA)	ISA1	0.958(0.832)	0.967 (0.943)	0.922 (0.853)
	ISA2	0.946(0.908)		
	ISA3	0.981(0.913)		

Table 4 shows that the loading of these items is higher than that of other items. These two steps prove the discriminant validity of the model. Therefore, all relevant tests have proved the model’s reliability and validity for the structural model’s evaluation (Sun, 2021; Sun, 2021). The before-test results are in bracket whereas the after-test results are without blanket.

Table 4
CORRELATION MATRIX AND SQUARE ROOTS OF AVE

Construct	1	2	3	4	5	6
PS	0.923 (0.819)					
PSU	0.322 (0.345)	0.901 (0.885)				
FE	0.152 (0.223)	0.231 (0.358)	0.933 (0.878)			
SE	0.016 (0.113)	-0.254 (-0.421)	0.188 (0.324)	0.948 (0.879)		
PE	0.498 (0.359)	0.409 (0.467)	0.222 (0.371)	0.052 (0.158)	0.876 (0.801)	
ISA	0.092 (0.186)	0.001 (0.217)	0.391 (0.477)	0.466 (0.519)	0.145 (0.247)	0.937 (0.904)

Note. The diagonal is the square root of the AVE value.

Figure 4 and Figure 5 shows PLS analysis results of the overall theoretical explanatory power of the model and estimated path coefficients. Table 5 shows obviously different effects between before and after tests. In the before-test, the relationships between perceived severity and response efficacy, perceived susceptibility and response efficacy, perceived severity and self-efficacy, fear and ISA are not significant. But in the after-test, not only all relationships are supported, but also all the t-values have increased. All the estimates’ p-value is less than 0.05, as well as the estimates’ p-value of between mediating factors and ISA are all less than 0.01, which indicates all the mediating factors are significant. The constructs have only explained a large proportion of the variance 20.3% in ISA in the before-test, whereas the same constructs have explained a large proportion of the variance 31.7% in ISA in the after-test.

Table 5
COMPARISON OF HYPOTHESES TESTING RESULTS

Hypotheses	Paths	Before		After	
		Estimate	t-value	Estimate	t-value
H1	Perceived Severity → Fear	0.409	4.326**	0.401	5.241**
H2	Perceived Susceptibility	0.277	3.053**	0.358	3.845**

Citation Information: Meng, C.Z., Yusoff, S.K.M., & Xian, B.S. (2021). Before-after investigation on bank information security drill: Severity, susceptibility and fear. *Journal of Management Information and Decision Sciences, 24*(S6), 1-13.

	→ Fear				
H3	Perceived Severity → Response Efficacy	0.087	0.648	0.352	3.189**
H4	Perceived Susceptibility → Response Efficacy	0.203	1.314	0.225	2.120*
H5	Perceived Severity → Self-efficiency	0.109	0.922	-0.307	2.584**
H6	Perceived Susceptibility → Self-efficiency	-0.324	2.182*	-0.261	2.291*
H7	Fear → ISA	0.057	0.410	0.324	2.847**
H8	Response Efficacy → ISA	0.302	2.442*	0.253	2.944**
H9	Self-efficiency → ISA	0.406	4.058**	0.358	3.060**

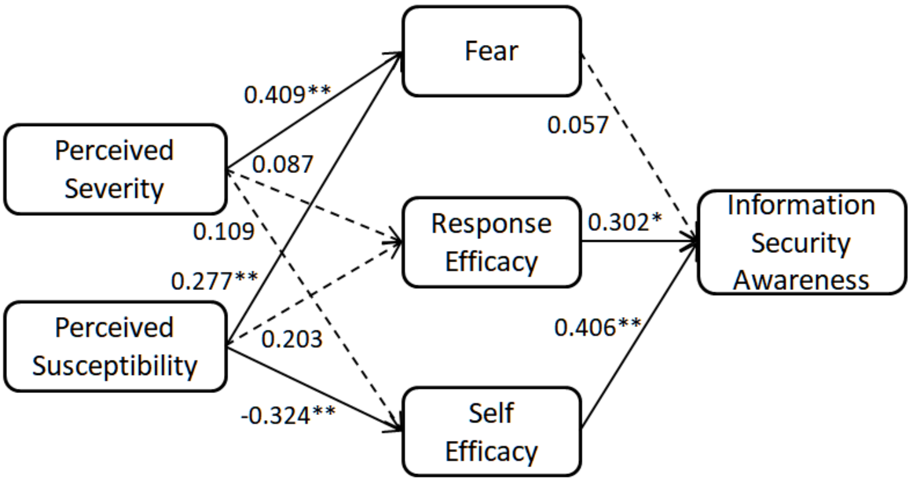


FIGURE 4
BEFORE TEST STRUCTURAL MODEL (NOTE: *P<0.05; **P<0.01)

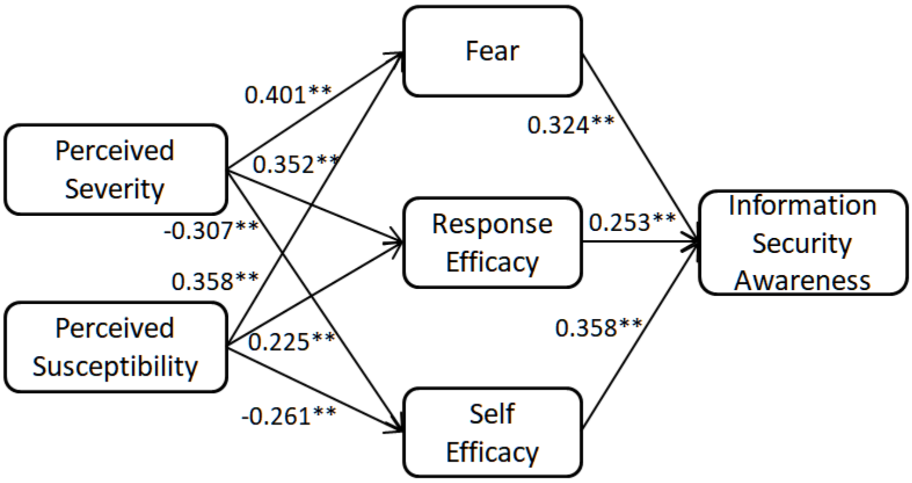


FIGURE 5
AFTER TEST STRUCTURAL MODEL (NOTE: *P<0.05; **P<0.01)

DISCUSSION

The comparative research results indicate that information security drill has produced better persuasion for bank employees. These findings contribute in study on how bank employees' belief and perspectives towards information security awareness. Taking into consideration the importance of EPPM theory in the before-after tests, this study proves that information security drills are necessary aids for information security training because it reduces costs as well as can be a good analogue of routines. Notably, most of the relationships of the before test are relatively low or not significant, whereas all the relationships are supported in the after test and the estimates relatively increased except the relationship between perceived susceptibility and self-efficacy. As expected, high perceived severity and perceived susceptibility positively affect fear, which indicates that bank employees with high perceived severity and susceptibility will fear more in dealing with malware. Increasing fear will be useful in increasing the bank employees' information security awareness. In addition, high perceived severity and perceived susceptibility positively affect response efficacy, which proves that bank employees with high perceived severity and susceptibility will show more efficacy in response to information security awareness. Moreover, perceived severity and susceptibility proves to negatively affect self-efficacy. When bank employees do not agree with the recommended action plan, even if we increase the degree of intimidation, they will not increase their enthusiasm for cooperation. It shows that high severity and susceptibility will decrease bank employees' self-efficacy in achieving more information security awareness.

CONCLUSIONS AND LIMITATIONS

It's important to turn a crisis experience into a useful coping technique (Shivaram, 2020), therefore, drills are useful crisis experience for information security training because they not only reduce the cost of training, but also do not take up too much time of employees. Many traditional employee training programs have been over-taught (Kala, 2020), but some efficient skills are not a sufficiently addressed at a certain level, such as drilling. The banks can retrieve the risk-resisting ability potential of their vocational education, knowledge popularization, staff training, daily demonstration and live exercise to reduce the financial and competing cost related with financial fraud, information theft and hacker attacks. Since quite a few of bank employees are on the road visiting clients on business negotiations with varieties of mobile devices, the banks should not only regularly upgrade office software to prevent malware attacks, but also should establish strict operation process and train employees in compliance with confidentiality. Additionally, establishing good relationships between companies and employees by offering regular communication can improve the employees' self-efficacy and response efficacy to information risks. Moreover, because too severe punishments will reduce the susceptibility of employees to risks, banks must draw up reasonable reward and punishment measures to motivate employees to self-discipline instead of bringing psychological pressure or fear to them. The bank can improve employees' risk prevention capabilities through training and drills. It is necessary to establish a complete internal training and drills system to enhance employees' risk management ability. Practicing drilling is relatively cheaper than long term training, which can be done several times per year. Bank employees can receive and experience the new malwares in the drill and learn how to deal with them. Research results indicate that experience with infection malwares can enhance bank employees' active defense behavior. It is therefore suggested that the banks can not only strengthen the application of emerging technologies in dealing with information security risks, but also reward employees to effectively help customers mitigate security and privacy violations. Overall, since there have been a large number of telecommunication network fraud cases in recent years, bank employees' crisis management capabilities must be improved through operational, functional and comprehensive training and drills. Overall, drill can test the bank's existing information security rules, improve the tacit understanding of various departments, and achieve the best results with less consumption.

This research had encountered some limitations which need to be taken into account. Companies in different financial industries such as insurance, trust, securities, have to be verified and compared in future researches. Future researches should also combine the cultural factors of different countries and regions with the characteristics of employees and psychological factors.

REFERENCES

Barth, S., Menno, D.T., de Jong, M.J., Pieter, H.H., & Janina, C.R. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics. 41*, 55-69.

Chen, Y.J., Wan, C.L., Yuh, M.C., & Jyun, H.W. (2019). Fraud detection for financial statements of business groups. *International Journal of Accounting Information Systems, 32*, 1-23.

Hajek, P., & Roberto, H. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud – A comparative study of machine learning methods. *Knowledge-Based Systems, 128*, 139-152.

Li, Z.dan., Wen, M.L., Qiao, Y.W., Jiageng, C., Wei, Y., & Kaitai, L. (2019). An efficient blind filter: Location privacy protection and the access control in FinTech. *Future Generation Computer Systems, 100*, 797-810.

Joon, B.S., Rebecca, N., & Richard, T. (2019). The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. *International Journal of Law, Crime and Justice. 56*, , Pages 79-88.

Rahouti, A., Lovreglio, R., Gwynne, S., Jackson, P., Datoussaid, S., & Hunt, A. (2020) Human behavior during a healthcare facility evacuation drills: Investigation of pre-evacuation and travel phases. *Safety Secience, 129*, 104754.

Steve, G., Martyn, A., Max, K., Noureddine, B., Karen, B.C. Natalie, Van.der.Wal, & Enrico, R. (2020). The future of evacuation drills: Assessing and enhancing evacuee performance. *Safety Science, 129*, 104767.

Spiteri, D., & Guoyuan, S. (2018). A comparison of student teachers' perceptions of school placement experience in Malta and China Compare. Compare. 888-904.

Hamilton, B., Ernest, B.R. (2017). Comparing Chinese undergraduate students' level of intercultural communication competence: Does studying in the USA make a difference? Compare. 283-297.

Gromada, A., Gwyther, R., & Yekaterina, C. (2019). Comparing inequality in adolescents' reading achievement across 37 countries and over time: outcomes versus opportunities. Compare.

Warwick, P., & Yvonne, J. (2013). A comparative study of perceptions of internationalisation strategies in UK universities. Compare. 102-123.

Elvik, R., Heidi, U., Kristina, W., Ragnhild, S., Syrstad, A.R., Seeberg, M.U., & Gulbrandsen, M.W. (2017). An empirical bayes before-after evaluation of road safety effects of a new motorway in Norway. *Accident Analysis and Prevention, 108*, 285-296.

Zheng, L., & Tarek, S. (2019). A full Bayes approach for traffic conflict-based before–after safety evaluation using extreme value theory. *Accident Analysis and Prevention*, *131*, 308-315.

Melissa, R., Bowers, J., Reggie, H., & Mandyam, M.S. (2017). Organizational culture and leadership style: The missing combination for selecting the right leader for effective crisis management. *Business Horizons. 60*, 551—563.

Kubiak, S., Daria, S., & Erin, C. (2019). Enhancing knowledge of adolescent mental health among law enforcement: Implementing youth-focused crisis intervention team training. *Evaluation and Program Planning. 73*. 44-52.

Waele, A.De., An-Sofie, C., & Michael, O. (2020). Preparing to face the media in times of crisis: Training spokespersons' verbal and nonverbal cues. *Public Relations Review*, *46*, 101871.

Miller, R.M., & Capaldi, E.J. (2005). An analysis of sequential variables in Pavlovian conditioning employing extended and limited acquisition training. *Learning and Motivation. 37*, 289–303.

Lucio, I., & Luca, C. (2005). Employing virtual humans for education and training in X3D/VRML worlds. *Computers & Education. 49*. 93–109.

Lefebvre A., J.F. Bassereau, A.M. Pensé-Lheritier, C. Rivère, N. Harris, R. Duchamp. (2009) Recruitment and training of a sensory expert panel to measure the touch of beverage packages: Issue and methods employed. Food Quality and Preference. 21. 156–164.

Han, J., Peter, H.N., Ashley, M., & Guid, O. (2011). Intelligent trainee behavior assessment system for medical training employing video analysis. *Pattern Recognition Letters*, *33*, 453–461.

Kramera, A., & Marcus, T. (2018). Does learning trigger learning throughout adulthood? Evidence from training participation of the employed population. *Economics of Education Review*, *62*, 82–90.

Jia Ya-hui, T.S., Shun, Y.W., Zhang, Q., & Yu, X.S. (2019). Discrete dynamics in nature and society.

Redmond, M.L., Fanglong, D., & Linda, M.F. (2015). Does the extended parallel process model fear appeal theory explain fears and barriers to prenatal physical activity? *Women's Health Issues*, *25*(2), 149-154.

Shi, J., & Sandi, W.S. (2015). The effects of fear appeal message repetition on perceived threat, perceived efficacy, and behavioral intention in the extended parallel process model. *Health Communication*.

Kotowski, M., Johnstone, P., Smith, S.W., & Pritt, E. (2011). Using the extended parallel process model to create and evaluate the effectiveness of brochures to reduce the risk for noise-induced hearing loss in college students. *Noise & Health*, *13*, 261–271.

Smith, S.W., Rosenman, K.D., Kotowski, M.R., Glazer, E., McFeters, C., Keesecker, N.M., & Law, A. (2008). Using the EPPM to create and evaluate the effectiveness of brochures to increase the use of hearing protection in farmers and landscape workers. *Journal of Applied Communication Research, 36,* 200–218.

Murray-Johonson, L., Witte, K., Liu, W.Y., Hubbell, A., Sampson, J., &Morrison, K. (2001). Addressing cultural orientations in fear appeals: Promoting AIDS-protective behaviors among Mexican immigrant and African American adolescents and American and Taiwanese collegestudents. *Journal of Health Communication, 6,* 335–358.

Witte, K. (1997). Preventing teen pregnancy through persuasive communications: Realities, myths, and the hard-fact truths. *Journal of Community Health, 22,* 137–154.

Moscato, S., Black, D.R., & Mattson, M. (2001). Evaluating a fear appeal message to reduce alcohol use among "greeks". *American Journal of Health Behavior, 25*(5), 481.

Wolburg, J. (2001). The "risky business" of binge drinking among college students: Using risk models for PSAs and anti-drinking campaigns. *Journal of Advertising, 30*, 23–39.

Zisserson, R.N., Palfai, T.P., & Saitz, R. (2007). "No-contact" interventions for unhealthy college drinking. *SubstanceAbuse, 28*,119–131.

Roberto, A.J., Meyer, G., Johnson, A.J., & Atkin, C.K. (2000). Using the extended parallel process model to prevent firearm injury and death: Field experiment results of a videobased intervention. *Journal of Communication, 50*, 157-175.

Witte, K., Berkowitz, J.M., Lillie, J.M., Cameron, K.A., Lapinski, M.K., & Liu, W. (1998). Radon awareness and reduction campaigns for African-Americans: A theoretically based evaluation. *Health Education & Behavior, 25*, 284-303.

Witte, K., Cameron, K.A., McKeon, J.K., & Berkowitz, J.M. (1996). Predicting risk behaviors: Development and validationof a diagnostic scale. *Journal of Health Communication, 1,* 317-341.

Lorenc, T., Clayton, S., Neary, D., Whitehead, M., Petticrew, M., Thomson, H., Renton,A. (2012). Crime, fear of crime, environment, and mental health and wellbeing:Mapping review of theories and causal pathways. *Health & Place, 18*(4), 757–765.

Omer, F., Malik, A.C.H., Schat, M.M.R., Asif, S., & Majid, K. (2018). Relationships between perceived risk of terrorism, fear, and avoidance behaviors among Pakistani university students: A multigroup study. *Personality and Individual Differences, 124*, 39–44.

Shin, S., Eyun, J.K., & Glenn, G.W. (2017). The effectiveness of fear appeals in 'green' advertising: An analysis of creative, consumer, and source variables. *Journal of Marketing CoMMuniCations, 23*(5),473–492

Gore, T.D., & Bracken, C. (2005). Testing the theoretical designof a health risk message: Reexamining the major tenets of theextended parallel process model. *Health Education & Behavior, 32*, 27 -41.

McMahan, S., Witte, K., & Meyer, J. (1998). The perception of risk messages regarding electromagnetic fields: Extending the extended parallel process model to an unknown risk. *Health Communication, 10*, 247-259.

Roberto, A.J., Meyer, G., Johnson, A.J., & Atkin, C.K. (2000). Using the extended parallel process model to prevent firearm injury and death: Field experiment results of a video based intervention. *Journal of Communication, 50*, 157-175.

Tay, R., Watson, B., Radbourne, O., De, Y.B. (2001). The influence of fear arousal and perceived efficacy on the acceptance and rejection of road safety advertising message. 2001: Road Safety Research, Policing and Education Conference (Regain the Momentum).

Lawson, S.T., Yeo, S.K., & Yu, H. (2016). *The cyber-doom effect: The impact of fear appeals in the US cyber security debate[C]*, International Conference on Cyber Conflict. IEEE, 2016.

Huang, H.T., Yu, M.K., Shiang, R.W., Chia, F.W., & Chung, H.T. (2016). Structural factors affecting health examination behavioral intention international *Journal of Environmental Research and Public Health. 13,* 395.

Sun, W., Dedahanov, A.T., Shin, H.Y., & Kim, K.S. (2019). Extending UTAUT Theory to Compare South Korean and Chinese Institutional Investors' Investment Decision Behavior in Cambodia: A Risk and Asset Model. *Symmetry. 11*, 1524.

Sun, W., Dedahanov, A.T., Shin, H.Y., & Kim, K.S. (2020). Switching intention to crypto-currency market: Factors predisposing some individuals to risky investment. *Plos One. 06*(04).

Sun, W., Dedahanov, A.T., Shin, H.Y., & Li, W.P. (2021). Factors affecting institutional investors to add crypto-currency to asset portfolios. *The North American Journal of Economics and Finance*. *58*(1), 101499.

Sun, W., Dedahanov, A.T., Shin, H.Y., & Li, W.P. (2021). Using extended complexity theory to test SMEs' adoption of Blockchain-based loan system. *PLoS ONE. 16*(2), 1-19.

Shivaram, V., Devarakonda, Jeffrey, J.R. (2020). Safeguarding from the Sharks: Board representation in minority equity partnerships. *Organization Science*. *30*(5).

Kala, C., Seal, L.A., Leon, Z.H., & Przasnyski, G.L. (2020). Delivering business analytics competencies and skills: A supply side assessment. INFORMS Journal on Applied Analytics, *50*(4).