The African Journal of Information Systems

Volume 15 | Issue 3 Article 3

October 2023

Assessing Employees’ Cybersecurity Attitude Based on Working and Cybersecurity Threat Experience

Norshima Humaidi
Universiti Teknologi MARA (UiTM), norshima958@uitm.edu.my

Melissa Shahrom
Universiti Teknologi MARA (UiTM), melissa@uitm.edu.my

Recommended Citation

Humaidi, Norshima and Shahrom, Melissa (2023) "Assessing Employees’ Cybersecurity Attitude Based on Working and Cybersecurity Threat Experience," *The African Journal of Information Systems*: Vol. 15: Iss. 3, Article 3.
Available at: https://digitalcommons.kennesaw.edu/ajis/vol15/iss3/3

Assessing Employees' Cybersecurity Attitude Based on Working and Cybersecurity Threat Experience

Research Paper

Volume 15, Issue 3, October 2023, ISSN 1936-0282

Norshima Humaidi
Faculty of Business and Management
Universiti Teknologi MARA
norshima958@uitm.edu.my

Melissa Shahrom
Faculty of Business and Management
Universiti Teknologi MARA
melissa@uitm.edu.my

(*Received March 2023, accepted September 2023*)

ABSTRACT

Many cybersecurity problems are caused by human error, which is a worry in the commercial sector. Due to their attitude towards cybersecurity, many employees in the firm do not work in a way that safeguards data. This study seeks to examine employees' cybersecurity attitudes with a focus on their work experience and exposure to cybersecurity threats. Data were gathered through a survey conducted in targeted business firms located in the Klang Valley area, Malaysia. Utilizing ANOVA and two-sample tests, the study analysed 245 data samples to evaluate the hypotheses. The results show significant distinctions in employees' cybersecurity attitudes in relation to the extent of their work experience and their previous encounters with cybersecurity threats. These findings hold valuable implications for the field of information security management, offering insights into how the industry can refine its strategic planning for information security. This can positively affect cybersecurity attitudes among employees within organizations.

Keywords

Cybersecurity attitude, cybersecurity threat, working experience, cybersecurity threat knowledge, information security, business management, information system, information technology.

INTRODUCTION

The Internet and related technology are evolving rapidly, and companies rely on these developments to carry out business activities, communicate and store data. As a result of this new business environment, companies operate digitally in cyberspace and this makes them vulnerable to cyberattacks. The impact of cyber-attacks is significant. In Malaysia, there are reported to have been on average 31 cybersecurity incidents each day; these include fraud, hacking, and data breaches (Meikeng, 2021). According to the 2022 Cost of a Data Breach Report by IBM, the average cost of a single data breach has risen to US$4.35 million (IBM, 2022). A survey of more than 5500 companies in 26 countries around the world by Kaspersky Lab revealed that 90% of organizations acknowledged security issue (Kaspersky Lab, 2022). Furthermore, 46% of firms reported that they had lost of sensitive data as a result of internal or external security breaches (Kaspersky Lab, 2022). The current research responds to this alarming rise in cybercrime. The key aim is to explore how employees' cybersecurity attitudes differ based on their working experience and cybersecurity threat experience. Employees are the users of any system implemented in an organization and they play a major role in protecting the information assets of the organization. Since the coronavirus disease 2019 (COVID-19) pandemic, many organizations have provided an option for employees to work from home. In the context of cybersecurity, employees' roles in safeguarding information assets are receiving more attention than before, especially in cases when the effectiveness of security technologies used to protect companies from cyberattacks has fallen short of expectations (Ho & Gross, 2021).

The way businesses respond to a data breach can significantly influence the value of their shares and their reputation, qualifying the breach as a cyber crisis and having additional long-term consequences for business continuity and resilience (Wang & Park, 2017). The majority of breaches are as a result of human error; not only it is expensive to recover lost data, but the security response often results in significant additional expenses (Kang et al., 2022). Thus, the communication of strategies related to cybersecurity incidents has emerged as a crucial topic for study and application. Conducting education and training for company employees to increase their information security knowledge and awareness is recommended (Aldawood & Skinner, 2018). Security education, training, and awareness (SETA) programs have been shown to assist in improving employees' attitudes towards adopting appropriate cybersecurity behavior (Kennedy, 2016). A SETA program addresses a wide range of topics and can significantly increase employees' capability to maintain cybersecurity. Such a program involves educating employees on how to use an organization's websites, systems, accounts, emails and social media effectively, as well as discussing good judgment, ethics and the need for awareness training. By implementing SETA, employees can learn how to prevent and respond to cybersecurity threats and to identify vulnerabilities so as to actively safeguard the organization's data and sensitive information.

Researchers stress the importance of management support in order to elevate employees' security awareness to required levels (Tsohou et al., 2009). For the SETA program to be executed successfully, and to help ensure that employees are able to adhere to specified procedures, top management must fully support the program (Wang et al., 2022; Tu & Yuan, 2014). The more support there is, the more resources will be made available for security-related issues (Herath & Rao, 2009). Additionally, studies show that if employees had previously encountered a cybersecurity danger, their attitudes towards adopting the necessary cybersecurity behaviors are enhanced (Haeussinger & Kranz, 2013). It has been found that those employees who have dealt with cyber risks before, exhibit greater caution when managing work on online platforms (Haeussinger & Kranz, 2013). The purpose of this study was to assess the cybersecurity attitudes of employees according to their level of work experience and previous exposure to cybersecurity threats.

LITERATURE REVIEW

Rapid development of technology has made cybersecurity challenges one of organizations' top concerns. Many organizations today use online-accessible digital technology to perform and manage their business processes. Therefore, developing a cybersecurity strategy is an essential part of organizational strategic planning and should address the cybersecurity behaviors of all the employees in the organization.

Cybersecurity is defined as "the process, capacity or capability whereby information and communication systems and the information collected therein are safeguarded against damage, unauthorized use, manipulation or exploitation" (Shaikh & Siponen, 2023, p. 2). In other words, cybersecurity entails the prevention of damage to, unauthorized use of or exploitation of information and may include the restoration of electronic information and communications systems (Perwej et al., 2021). Tyagi (2019) claim that cybersecurity is a defense against cyberattacks for internet-connected systems and related data, software, and hardware.

Meanwhile, in a computing context, measures to improve both cybersecurity and physical security are employed by businesses to prevent illegal access to databases and computerized systems (de Gusmão et al., 2018). Since an organization's information assets are valuable and confidential, they need to be secured; exposing them to unauthorized users could endanger the business. Employees play an important role in protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction provided they use information technology effectively and adopt safe operating practices, that is, adhere to good cybersecurity behaviors, when working offline or online (Gillam & Foster, 2020).

Cyber Security Threat

'Cyber security threat' is a broad term encompassing any malicious activity involving stealing or damaging data, or causing disruptions in the digital ecosystem, whether this affects individuals, groups, or entities in general (Ghelani, 2022). These threats can manifest as denial-of-service attacks, phishing schemes, data breaches, and other tactics designed with the sole purpose of disrupting digital operations or compromising data integrity (Chang & Coppel, 2020). Typically, these threats are hostile actions intended to create disturbances and, while the cybercriminals are usually motivated by expectations of financial gain, such attacks often carry an additional malicious intent of inflicting harm on their targets (Sudhakar & Kumar et al., 2020). Business performance can be impacted by cybersecurity threats. Over time attacks have become increasingly sophisticated and frequent, especially since technologies have been evolving rapidly. Unfortunately, hackers have a good understanding of how to use these technologies and exploit the vulnerabilities of the digital systems (Perwej et al., 2021).

Cybercrime is sometimes described in terms of the crime triangle which asserts that three elements must be present for a cybercrime to take place: a victim, a motive, and an opportunity (Dhanjani et al., 2009). The person who will be attacked is the victim. The reason why the crime will be committed is the motive, and the time will be the opportunity. Cybercrimes or cyber threats are anything that can take advantage of a weakness in an organization's security system to damage, eliminate, or adversely impact an item or things of interest. In is increasingly evident that the infrastructure of an organization cannot be protected solely by technology. It is essential that organizations remain alert and put in place ways to regulate and monitor cyber threats. Hence, employees should be actively involved in protecting the organization's information assets.

In the information security literature, the classification of threats to information security is extensive. Guo (2013) divided information security threats into four categories: sources, perpetrators, intent and consequences. Sources can be internal or external to the organization, perpetrators can be human or non-human, intent can be intentional or unintentional (accidental), while consequences include data disclosure, data modification, data destruction, and denial of service. Natural disasters and human errors (entry of erroneous data by employees and accidental deletion or modification of data by employees) or omissions are examples of unintentional threats, whereas intentional threats include behaviors like computer fraud, embezzlement, and theft. Narayana Samy et al. (2010) propose a different categorization of threats to information security:

- Natural (in line with other studies that record natural catastrophes such floods, earthquakes, tornadoes, landslides, and electrical storms)
- Humans (unethical and deliberate acts)
- Environmental (pollution, chemical spills, and liquid leakage)

The organization can usually manage technology-related problems with ease. However, if not carefully monitored the problem of human error can be difficult to manage as it is complex (Gillam & Foster, 2020; da Veiga et al., 2020).

Numerous cyberattacks take place every day, and what is most concerning about them is that insiders are frequently involved directly or indirectly in helping cybercriminals to gain information about the target organization. The cyberattacks are frequently either carried out by employees of the targeted organization or facilitated by employees who give useful information to external attackers (Perwej et al., 2021). Security incidents created or facilitated by an internal party are difficult to prevent and insider attacks are often more challenging to identify than the activities of an external hacker. (Corallo et al., 2020; Kennedy, 2016; Flores & Ekstedt, 2015). This is because employees have legal and frequently privileged access to facilities and organizational information, possess knowledge of the organization and its processes, and know where valuable or important assets are located. Employees who intend to exact revenge or to seek financial advantage are the perpetrators of malicious internal threats whereas errors made unintentionally by employees are non-malicious internal threats (van der Kleij et al., 2022). Many organizations are not aware that internal threats, for example identity theft from the organization's data and information destruction, can result in security issues.

In order to address information security concerns, an organization must invest more in human capital than in technology (Gillam & Foster, 2020). Without the right training and knowledge regarding information security, those who work for the organization and deploy technology will not be able to use it properly (da Veiga et al., 2020).

While not all cyber threats will stop businesses from operating, they are always inconvenient and reduce business productivity (Funk, 2022). Commercial information assets are valuable for enhancing business performance and security incidents are expensive. At first glance, it could seem that this only involves a loss of data, but the long-term costs could be much higher. For some firms the damage involves a minor increase in overall information technology spending, but for others there is major financial and reputational harm. In the worst case, it entails going out of business with all assets lost. The ability to reduce risk and avoid the uncertain path of recovery pays off since the cost of a security breach is higher than the cost of protection. Malik et al. (2022) stated that security incidents, such as data loss, loss of integrity and availability, or confidentiality breaches, can have both legal and practical impacts. Hence, business organizations need to take the threat posed by cybersecurity seriously and develop measures to raise employees' awareness of the issue.

Cybersecurity Attitude and Working Experience

Employees' cybersecurity attitude in this study refers to employees' belief in the effectiveness of complying with cybersecurity policies and practicing good security behavior. A person's experience is gained through participation in or exposure to an event to a certain extent. The individual's attitude, abilities, knowledge, and skills are all linked to experience and can be developed through formal or informal education supported by the top management in the organization (Shaikh & Siponen, 2023; Hadlington, 2018). Research by Hwang et al. (2019) claimed that employee security awareness was found to be linked to the employee's own observations and experiences related to workplace security. Security awareness results from both objective and subjective security experiences at work. Awareness encompasses not only conscious awareness of stimuli at the time of the experience, but also lessons learned from events in the past being related to the present, and projected on to the future (Hwang et al., 2019). Therefore, employees' experiences with previous and current security programs affect their knowledge of security awareness, and lead to a positive attitude towards complying with cybersecurity policies.

The study reported on here considers that the employees' working experiences when handling information systems (IS) that have been implemented in the organization to process business records play a major role in reducing security incidents. Such experience includes firsthand knowledge of information security incidents, information security training, and understanding the consequences of not complying with information security policies.

All employees need to be informed about their responsibility for protecting organizational data and information (Ani & He, 2018). In addition to their usual roles at work, they need to use the security mechanisms in place and foresee threats and appreciate the user benefits of guarding against data breaches. As they have a good ability to absorb new information, employees with substantial work experience are usually aware of the reasons for escalating security concerns (Szczepaniuk & Szczepaniuk, 2022). Hence more experienced employees will set a good example in practice and increase the resilience of the organization (Wong et al., 2022). However, those with lower previous exposure to cybersecurity issues must be provided with information security training so as to gain a basic grasp of the severity of this matter.

Furthermore, workers with existing work experience can be expected to adhere to the established security standards in the organization and also to stay current with new innovations including the regular introduction of sophisticated security tools from diverse sources. Highly experienced workers are expected to have a positive cybersecurity attitude and hence to be conscientious regarding adopting sound security practices. Also, because of their good absorptive capacity and because they are very familiar with the organization's information systems, they may not need the much technical support when executing their professional activities or dealing with security threats. Based on the above, this study postulates the following hypothesis:

H1: There are significant differences between cybersecurity attitudes of employees based on their working experience.

Cybersecurity Attitude and Cybersecurity Threat Experience

The first line of defense for an organization is its employees (Ho & Gross, 2021). The organization is in danger if the employees are unable to respond in a cybersecurity-aware manner. Employees need to be aware of the likelihood that there could be information security threats to their organization, as well as the potential repercussions for both the employees and the organization as a whole (Ani & He, 2018). Moreover, employees must be able to recognize information security dangers so that they can modify their behavior and course of action (Ameen et al., 2021). Previous studies have found that security problems may occur if employees are unaware of either the vulnerability of the organization to cyber-attacks or are unable to detect evidence that attempts have been made to gain unauthorized access to data or systems and this will increase cyber risk (Corallo et al., 2022; da Veiga et al., 2020).

The employees' cybersecurity attitude is influenced by information security knowledge as well as elements like culture and personality. Cybersecurity attitude is very important for improving information security awareness (Khando et al., 2021). Existing literature (such as Pósa and Grossklags, 2022) has indicated that in some instances early, formal, education-related security experiences, which build on early childhood behaviors, as well as experience from extended periods of full-time employment, are related to the development of strong security practices. It is extremely difficult to defend organizational systems against the various threats that attackers deploy to steal organization data without sufficient training and exposure of the employees to cybersecurity threats. Based on this, the following hypothesis has been constructed:

H2**:** There are significant differences between cybersecurity attitude of employees based on their cybersecurity threat experience.

RESEARCH METHODOLOGY

The respondents in this study were divided into four groups: (1) less than one year; (2) one to five years; (3) six to 10 years; and (4) more than 10 years. Based on the length of the employees' working experience with the company, we conclude that employees who had been working for more than ten years were placed in the group of highly experienced users, whilst those with less than ten years working experience were classified as less experienced users. Less experienced employees were referred as 'newborn babies' who require bottle feeding from top management to gain an understanding of the system environment quickly. Meanwhile, highly experienced employees were recognized for their ability to understand, and hence deal with, implicit features of security threats and to adjust to the speed of innovation (absorptive capacity). In addition, highly experienced employees were expected to have a positive cybersecurity attitude which is required when coping with new developments, such as updates of tools. Both absorptive capacity and cybersecurity attitude are attributes that are associated with effective protection of information assets.

Target respondents for this study were employees who work in various business sectors in the Klang Valley area in Malaysia. In identifying suitable respondents for the study, purposive sampling was used. This sampling technique helps researchers to choose a sample which is representative of the entire population. GPower software was used to calculate the minimum sample size. Since this study only focused on three variables (cybersecurity attitude, cybersecurity threat experience and working experience), with a small effect size (0.15) and the power needed at 0.95, the minimum sample size required was 119. However, a total of 245 responses were collected from the survey posted online and delivered in person. For the online survey, SurveyMonkey (https://www.surveymonkey.com/) was used in preparing the questionnaire and the URL link was shared via social media platforms (Facebook and WhatsApp). The items used to measure cybersecurity attitude were adapted from Hadlington (2017). The original items have been validated previously but were modified slightly for the present study. According to Saunders et al. (2019), the use of an established instrument is highly recommended as it enables subsequent comparison with other research. Additionally, the use of an established instrument can save the researchers time and effort required when a new instrument is developed (Sekaran & Bougie., 2016).

The respondents selected options for the items using a 5-point Likert scale: (1) strongly disagree to (5) strongly agree. Ethical issues were considered and included a statement of confidentiality and informed consent for participants. The data analysis began with data cleaning and normality testing and continued by analyzing the profiles of the respondents using IBM SPSS Statistics (Version 26). The objectives of this study were to test differences of cybersecurity attitude based on the respondent' level of working experience and cybersecurity threat experience. Thus, independent *t*-test and one-way analysis of variance (ANOVA) analyses were conducted using Excel software. The findings are explained in the next section.

RESEARCH FINDINGS

Respondents' Demographic Details

This study collected 245 sets of data from the target respondents for final analysis. Based on the demographic details result (see Table 1), the majority of the respondents were female (55.9%) compared to male (44.1%). Most of the respondents were 40 years old or younger (86.5%) with only 33 respondents older than 40 years of age (13.5%). Most of the respondents came from the education sector (23.7%), followed by finance or banking (18.4%), and then transport or automotive (11.4%). The highest level of education of most respondents was a bachelor's degree (55.5%), followed by diploma (22.9%), master's degree (11%), professional degree (4.9%), a few respondents had only completed primary and secondary levels of education (1.6%).

In terms of job position, 30.6% respondents were at executive level and 26.1% respondents were at a managerial level. Other positions selected were academicians (23.7%), low level position (3.7%) and others (15.9%). The majority of the respondents had 10 years or less of working experience (60%) compared with 40% respondents with more than 10 years of working experience. The majority of the respondents (68%) stated that they had experienced cybersecurity threats, while 38% of the respondents had no experience with cyber- attacks (Table 2). The details of the respondent's profile are presented in Table 1 and Table 2.

Table 1

Demographic Details

Demographic Variable	Frequency	Percentage
Gender		
Male	108	44.1
Female	137	55.9
Age		
Less than or equal to 40 years old	212	86.5
More than 40 Years old	33	13.5
Type of Industry		
Education	58	23.7
Utilities	19	7.8
Construction	10	4.1
Health	13	5.3
Finance/Banking	45	18.4
Transport/Automotive	28	11.4
Manufacturing	11	4.5
Media	5	2.0

Demographic Variable	Frequency	Percentage
ICT	6	2.4
Food	10	4.1
Electric and Electronic	4	1.6
Other	36	14.7
Qualification		
Professional Certificate	2	0.8
Diploma	56	22.9
Advanced Diploma	6	2.4
Bachelor Degree	136	55.5
Professional Degree	12	4.9
Master Degree	27	11.0
PhD	2	0.8
Other	4	1.6
Position		
Administrative Staff	9	3.7
Executive Level	75	30.6
Assistant Manager	10	4.1
Manager	18	7.3
Senior Manager	25	10.2
Assistant Engineer	1	0.4
Engineer	9	3.7
Senior Engineer	1	0.4
Academic Staff/Academician	58	23.7
Other	39	15.9
Working Experience		
Less than or equal to 10 years	147	60.0
More than 10 years	98	40.0

Table 2

Cybersecurity Threat Experience

Questions	Yes	%	No	%
Do you have any experience with cybersecurity threat?	152	62.0	93	38.0
Do you use mobile device for work purpose?	220	89.8	25	10.2

Reliability Analysis

This study used the Anova-two-factor without replication analysis tool to test the Cronbach's alpha reliability coefficient of the instrument. According to George and Mallery (2003), the Cronbach alpha value rules of thumb were "_ > .9 – Excellent, _ > .8 – Good, _ > .7 – Acceptable, _ > .6 – Questionable, _ > .5 – Poor, and < .5 – Unacceptable" (p. 231). The Cronbach's alpha value for cybersecurity attitude was 0.77, which is acceptable.

Descriptive Analysis

Skewness and kurtosis were measured to test the normality of data. The value of skewness for cybersecurity attitude was 0.238. This indicated that the data sample was positively skewed and relatively symmetric. Meanwhile, the value of kurtosis for cybersecurity attitude was 0.840, which is less than 3. This indicated that the sample data curve was flat with a wide degree of dispersion (Evans, 2017). The details of the descriptive analysis results can be found in Table 3.

Table 3

Cybersecurity Attitude Descriptive Analytics

Measurement	*Result Value*
Mean	3.667
Standard Error	0.027
Median	3.700
Mode	3.500
Standard Deviation	0.428
Sample Variance	0.183
Kurtosis	0.840
Skewness	0.238

The averages (mean), and standard deviations were calculated for each of ten items item related to cybersecurity attitude. The items' mean scores were greater than 3.0, except for item number 7 (mean value = 2.947) and item number 9 (mean value = 2.976) which were very close to 3. Item 7 asked whether the respondent was worried that if they reported a cyberattack incident to the police it would damage the reputation of the company. The majority of the respondents disagreed with this statement. Meanwhile, Item 9 asked whether the employee does *not* know how to report the cyberattack if it happened. Based on the mean, the majority of respondents were aware of cyberattacks and knew how to report cyberattack incidents occurring in their organizations. Moreover, many of the respondents were aware of their role and responsibility in keeping the company protected from cybercrime. This indicated that the organizations employing respondents had played the expected role and effectively implemented a SETA. The standard deviation results showed that the majority of respondents' data are close to the mean value. The overall results of descriptive analytics can be seen in Table 4.

Table 4

Descriptive Analytic for Employee's Cybersecurity Items – Mean and Standard Deviation Score Result

Items Code	Cybersecurity Attitude	*M*	*SD*
CA1	I am aware of my role in keeping the company protected from potential cyber criminals.	4.302	0.804
CA2	I believe everyone in the company has a role to play in protecting against threats from cyber criminals.	4.008	0.810
CA3	It is hard to know how I can help protect the organisation from cybercrime.	3.392	0.826
CA4	I don't have the right skills to be able to protect the organisation from cybercrime.	3.024	1.086
CA5	I do not feel that IT security is a priority within my organisation.	4.200	0.728
CA6	I think that reporting cybercrime is not waste of time.	4.237	0.696
CA7	I worry that if I report a cyberattack to the Police it might damage the reputation of my company.	2.947	0.845
CA8	I think more could be done to communicate the risks from cybercrime to individuals in the organisation.	3.927	0.796
CA9	I would not know how to report a cyberattack if one happened.	2.976	1.112
CA10	I don't think that reporting a cyberattack on the company is my responsibility.	3.660	0.777

In this study the cybersecurity attitude scores were divided into three ranges: (1) Low (mean value from 1.0 to 2.6), (2) Moderate (mean value from 2.7 to 3.6) and (3) High (mean value from 3.7 to 5.0). Based on the descriptive-analytic result (see Table 5), the level of cybersecurity attitude among the employees is high (n = 125) or moderate (n = 117) with few employes at the low level (three) (see Table 5).

Table 5

Average Scales for Employees' Cybersecurity Attitude

Level of Mean Score	Low (1 to 2.6)	Moderate (2.7 to 3.6)	High (More than 3.6)	Total Sample
Total	3	117	125	245

Hypothesis Testing

Two hypotheses were constructed for this study. The first compared the mean of cybersecurity attitude among the employees based on their different working experiences to determine whether all groups were similar or if there were significant differences. Four levels of working experience were tested: (1) Less than one year, (2) one to five years, (3) six to 10 years, and (4) More than 10 years. One-way ANOVA test analysis was used to test Hypothesis 1 (H1) (see Table 6). Based on ANOVA results (see Table 6), the *f*-value (417.647) is greater than the F_{crit} value (3.861). Meanwhile, the *p*-value (0.00) was less than 0.05. Therefore, we can conclude that there was a significant difference between the cybersecurity attitude of employees based on their working experience, hence Hypothesis 1 (H1) was accepted.

Table 6

One-Way ANOVA Analysis Result

Hypothesis	Variables	Average	Variance	*f*	*p*	F_{crit}
H1: There are significant different between cybersecurity attitude of employees based on their working experience.	Cybersecurity Attitude	3.667	0.183	417.647	0.000	3.861
	Working Experience	2.486	0.636			

Note. ANOVA = analysis of variance.

Furthermore, the difference in cybersecurity attitudes among the employees was tested based on cybersecurity threat experience. The respondents were divided into two groups: (1) those with cybersecurity threat experience (Yes) and (2) those without cybersecurity threat experience (No). A two-sample hypothesis test was used (see Table 7) and the results indicated that the *t*-statistical value (24.415) was higher than the critical value (1.651). Meanwhile, the *p*-value (0.00) was less than 0.05. It can be concluded that there was a significant difference between the cybersecurity attitudes of employees based on their cybersecurity threat experience. Hence Hypothesis 2 (H2) was accepted.

Table 7

Two-Sample Hypothesis Test Analysis Result

		Average		Variance				
Hypothesis	Variables	Yes	No	Yes	No	Critical Value	*t*	*p*
H2: There are significant different between cybersecurity attitude of employees based on their cybersecurity threat experience.	Cybersecurity Threat Experience	3.719	3.636	0.213	0.163	1.651	24.415	0.000

DISCUSSION

Cybersecurity is critical in today's digitally driven world as a way to defend enterprises from cybersecurity risks. Hence, employee attitudes to cybersecurity are critical to the entire security situation in the organization (Hadlington, 2018). According to the data collected in the study reported on here, there are considerable variances in employees' cybersecurity views based on their job experience. This agrees with the findings of Kennison et al. (2021) that, because of their exposure to security practices, experienced personnel frequently have a superior understanding of cybersecurity Furthermore, employee contacts with dangers, such as becoming a victim of phishing, can make employees more careful about their online activity. These people are likely to follow well-established cybersecurity policies and best practices.

Direct encounters with cybersecurity threats can have a major impact on an employee's attitude. Those who have been victims of cyberattacks may be more aware of the dangers involved (Alanazi et al., 2022). These encounters can inspire a proactive and cautious approach to cybersecurity. Because they have watched the sector change, more experienced individuals tend to have a good understanding of cybersecurity fundamentals. Meanwhile, staff with less experience may be technically proficient but less mindful of potential hazards.

IMPLICATIONS

Organizations might think that providing information on security is not necessary in their organization because they do not have sufficient information or information access is difficult. The study reported on here was undertaken to demonstrate the implications of employees' cybersecurity attitude to the organization. According to the current findings, employee attitudes collectively contribute to the cybersecurity culture of the organization, and experienced employees can serve as role models for cybersecurity best practices. Employees with more experience can mentor their younger colleagues, promoting a culture of security knowledge and responsibility.

A strong cybersecurity culture is essential for overall security effectiveness. Corallo et al. (2022) suggest that the organization should develop an awareness and training or SETA program to improve employees' cybersecurity attitudes. This type of program is important as it can improve employees' attitudes towards practicing good cybersecurity protective behavior. The SETA should be conducted annually, and attendance should be made compulsory for all employees in the organization regardless of their position in the organization. During the program, the employees may be required to participate in practical exercises so that they understand the procedures well when implementing them. The risk of data breaches can be reduced by highlighting what the employee should do in dealing with such problems, and the exercises help develop problem-solving skills (Szczepaniuk & Szczepaniuk, 2022).

Learning how to safeguard data is crucial, as this reduces the chances of threats to the organization succeeding, such as ransomware and email phishing, which is linked to due to human error. It is also suggested that employees be tested based on the material that has been covered in the training. In addition, gathering feedback from them is essential to assist the organization to improve the training program and to make it more effective in the future (Alanazi et al., 2022). Security awareness has been shown to improve employees' attitude, leading to a change for the better in security behavior. If employees intend to misuse or abuse information they could be charged with penalties (Hadlington, 2017). An effective SETA program is the most effective way to combat this issue.

Appropriate control to maintain a fundamental degree of security, and a monitoring system to keep an eye out for policy violations, are essential components of an efficient cybersecurity plan. All employees should undergo information security training to help them gain experience and grasp the best practices for data management, security and disposal. Organizations should ensure that their employees have the information, awareness, and the abilities necessary to contribute to the organization's defense against cyberattacks and data breaches. Therefore, management plays an important role in providing sufficient knowledge about information security to all employees by conducting information security training and education and implementing security awareness programs or campaigns effectively.

Furthermore, employees should be part of security strategic planning, especially employees who work with sensitive and confidential data as they will get a fully informed view of organizational security planning and the importance of being very aware of emerging cyber threats that can attack the company.

CONCLUSION

Every person in the organisation is responsible for protecting the organisation's information assets. However, top management plays a particularly important role in establishing security regulations and ensuring that the employees are aware of the current risks and strategies. Individuals, particularly ordinary people, may not be particularly knowledgeable about computers and, without the necessary expertise, might become harmful to an information system or the data belonging to the organization. Hence, SETA programs will be an effective and systematic way of training, educating, and raising awareness about security and data protection. As a result, employees may become more security aware and aware of security concerns, and this will decrease the number of security incidents. This could also protect the organisation and any data or information associated with the user or organisation.

Data breaches and unauthorized access to important information may disrupt the normal business of the organisation if it is not taken seriously. Information security not only keeps the information safe, but has wide-ranging benefits for employees, clients, and the company as a whole, for example, business continuity would not be endangered. Strong information security reduces the risk of both internal and external attacks. It is the responsibility of those on positions of authority to ensure that the employees and people outside the organization but using its systems, know how to avoid information disclosure. This is done with the help of awareness programs and training. Not all organisations implement such programs sufficiently frequently, but need to become convinced that this is an effective way to solve information security issues. Resources should also be allocated for information security. Visible support from management plays a role in motivating employees to implement and adhere to the security measures. Constant reminding by means of awareness and training, of the importance of data security and the consequences of data breaches to the organisation remains crucial.

Crucially, people need to become aware of information security. This can be achieved in various ways though some of these are costly. Combining both traditional and digital methods (for instance using a mixture of video, advertisements, newsletters, or posters) could assist in making systems users aware of information security. A firewall alone is not enough to protect information within the organisation. This is because firewalls have their limitations, and they cannot easily adapt to rapidly changing situations. A firewall is not innately intelligent and as is operated and configured by people, so it can be expected on occasion to be affected by a mistake made by a human operator or end-user. The configuration and management of firewalls requires a certain amount of expertise.

To conclude, whether it is a small, a medium or a large organisation, information security issues should not be taken lightly. If the organisation has not started implementing security measures, this is a starting point for them. Additional, technological aspects security management can be addressed using anti-malware, a virtual private network, and biometrics. To manage costs for the maintenance contracts, a budget should be allocated to include technology being used. In integrating the efforts, organisations at large may save themselves from more serious information security issues.

REFERENCES

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Aldawood, H.A., & Skinner, G. (2018). A critical appraisal of contemporary cybersecurity social engineering solutions: Measures, policies, tools and applications. In *Proceedings of the 2018 26th International Conference on Systems Engineering (ICSEng)*, Sydney, Australia (pp.1–6). IEEE. https://doi.org/10.1109/ICSENG.2018.8638166

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114,* 106531 1–19. https://doi.org/10.1016/j.chb.2020.106531

Ani, U. P. D & He, H. (2018). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2–35. https//doi.org/10.1108/JSIT-02-2018-0028

Chang, L. Y., & Coppel, N. (2020, October). Building cybersecurity awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Corallo, A., Lazoi, M & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry, 114,* 103165. https://doi.org/10.1016/j.compind.2019.103165

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review. *Computers in Industry, 137,* 103614. https://doi.org/10.1016/j.compind.2022.103614

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

de Gusmão, A. P. H., Silva, M. M., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, *43,* 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Dhanjani, N., Rios, B., & Hardin, B. (2009). *Hacking: The Next Generation*. O'Reilly Media, Inc.

Evans, J.R. (2017). *Business Analytics: Methods, Models, and Decisions* (2nd ed.). Pearson Education Limited.

Flores, W., & Ekstedt, M. (2015). Exploring the link between behavioural information security governance and employee information security awareness. In S. M. Furnell & N. L. Clarke (Eds.), *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* (pp. 82–94). Plymouth University.

Funk, P. (2022). Artificial intelligence and cybersecurity implications for business management. *Journal of International Scientific Publications, Economy & Business, 16,* 252–261. https://www.scientific-publications.net/en/article/1002435/

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. https://doi.org/10.1177/1460458210377468

George, D., & Mallery, P. (2003). *SPSS for Windows Step by Step: A Simple Guide and Reference. 11.0 update* (4th ed.). Allyn & Bacon.

Ghelani, D. (2022). Cybersecurity, cyber threats, implications and future perspectives: A review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19 https://www.authorea.com/doi/full/10.22541/au.166385207. 73483369

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, *108*, 1–12. https://doi.org/10.1016/j.chb.2020.106319.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace. *Computers and Security, 32,* 242–251. https://doi.org/10.1016/j.cose.2012.10.003

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. J. (2018). Employees attitudes towards cybersecurity and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269–281. https://doi.org/10.5281/zenodo.1467909

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. In *ICIS 2013 Proceedings*. Association for Information Systems. https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/9

Herath, T., & 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

Ho, S. M & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. *Computers and Security, 108,* 102357. https://doi.org/10.1016/j.cose.2021.102357

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems, 61*(4), 345–356. https://doi.org/10.1080/08874417.2019.1650676

IBM (2022). Cost of a data breach 2022 Report. Retrieved 21 December 2022. https://www.ibm.com/reports/data-breach

Kang, P., Kang, J., & Monsen, K.A. (2022). Nurse information security policy compliance, information competence, and information security attitudes predict information security behavior. *Computers, Informatics, Nursing, 41*(8), 595–602. https:doi.org/10.1097/CIN.0000000000000981

Kaspersky Lab (2022*). Damage Control: The Cost of Security Breaches,* IT Security Risks Special Report Series. Retrieved 10 October 2023 https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Kennedy, S. E. (2016). The pathway to security: Mitigating user negligence. *Information & Computer Security*, *24*(3), 255–264. https://doi.org/10.1108/ics-10-2014-0065

Kennison, S. M., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports*, *4*, 100132. https://doi.org/10.1016/j.chbr.2021.100132

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Malik, A.W., Abid, A., Farooq, S., Abid, I., Nawaz, N.A., & Ishaq, K. (2022). Cyber threats: taxonomy, impact, policies and way forward. *KSII Transactions on Internet and Information Systems*, *16*(7), 2425-2458. https://doi.org/10.3837/tiis.2022.07.017

Meikeng, Y. (2021, Sept 19). Online threats continue to spike. *The Star* Retrieved from The Star: https://www.thestar.com.my/news/focus/2021/09/19/online-threats-continue-to-spike

Perwej, Y., Abbas, S. Q., Dixit, J. P., & Akhtar, N. (2021, December 28). A systematic literature review on the cybersecurity. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Pósa, T., & Grossklags, J. (2022). Work experience as a factor in cyber-security risk awareness: A survey study with university students. *Journal of Cybersecurity Privacy. 2*(3), 490–515. https://doi.org/10.3390/jcp2030025

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students.* Pearson Education Limited.

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security, 124,* 102974. https://doi.org/10.1016/j.cose.2022.102974

Sudhakar, & Kumar, S. (2020, January 14). An emerging threat Fileless malware: A survey and research challenges. *Cybersecurity*, *3*(1), 1-12. https://doi.org/10.1186/s42400-019-0043-x

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy,* *46*(3), 102282. . https://doi.org/10.1016/j.telpol.2021.102282

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2009). Aligning security awareness with information systems security management. In *MCIS 2009 Proceedings.* Association for Information Systems. https://aisel.aisnet.org/mcis2009/73

Tu, Z., & Yuan, Y. (2014). *Critical success factors analysis on effective information security management: A literature review.* Unpublished dissertations, McMaster University. Available at https://macsphere.mcmaster.ca/handle/11375/18168

Tyagi, S. (2019). Cybercrime overwhelming online banking: A project management approach's alternative. *PM World Journal, VIII(V),* 1-21. Retrieved from https://pmworldlibrary.net/wp-content/uploads/2019/06/pmwj82-Jun2019-Tyagi-cybercrime-overwhelming-online-banking.pdf

van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security, 113,* 102535. https://doi.org/10.1016/j.cose.2021.102535

Wang, G., Tse, D., Cui, Y., & Jiang, H. (2022). An exploratory study on sustaining cybersecurity protection through SETA implementation. *Sustainability*, *14*(14), 8319. https://doi.org/10.3390/su14148319

Wang, P., & Park, S.-A. (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems*, *18*(2), 136-147.

Wong, L-W., Lee, V-H, Tan, G. W-H, Ooi K-B & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520