ISSN: 2456-043X

International Journal of Engineering Science and Generic Research (IJESAR)

Available Online at www.ijesar.in

Volume 11; Issue 4; 2025; Page No. 33-46

Evaluating Employees' Cybersecurity Perspectives Informed by Professional and Cybersecurity Threat Experiences

Sourabh Singh, Sanjeev Kumar Sharma

Department of CSE, Sunrise University, Alwar Rajasthan

Article Info: Received: 11-03-2024 / Revised: 22-04-2024 / Accepted: 28-05-2025
Correspondence: Sourabh Singh
Conflict of interest statement: No conflict of interest

Abstract

A significant number of cybersecurity issues stem from human mistake, posing a concern in the business sector. Many personnel in the organization do not engage in practices that protect data due to their attitude towards cybersecurity. This research aims to investigate workers' cybersecurity perceptions, emphasizing their professional experience and exposure to cybersecurity dangers. Data were collected via a survey administered at selected business enterprises situated in the Klang Valley region of Malaysia. The research used ANOVA and two-sample tests to analyze 245 data samples for hypothesis evaluation. The findings reveal notable differences in workers' cybersecurity attitudes based on their level of work experience and prior exposure to cybersecurity dangers. These results possess significant implications for information security management, providing insights into how the industry might enhance its strategic planning for information security. This may enhance cybersecurity perceptions among personnel inside firms.

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

Introduction

The Internet and other technologies are advancing swiftly, and enterprises depend on these innovations to conduct corporate operations, communicate, and store information. The modern corporate climate compels organizations to function digitally in cyberspace, rendering them susceptible to cyberattacks. The ramifications of cyber-attacks are substantial. In Malaysia, an average of 31 cybersecurity events occur daily, including fraud, hacking, and data breaches (Meikeng, 2021). The 2022 Cost of a Data Breach Report by IBM indicates that the average cost of a single data breach has increased to US$4.35 million (IBM, 2022). A Kaspersky Lab study of over 5,500 enterprises across 26 countries indicated that 90% of organizations recognized security concerns (Kaspersky Lab, 2022). Moreover, 46% of companies said that they have experienced the loss of sensitive data due to internal or external security breaches (Kaspersky Lab, 2022). This paper addresses the concerning increase in cybercrime. The primary objective is to investigate the variations in workers' cybersecurity attitudes contingent upon their professional experience and exposure to cybersecurity threats. Employees are the users of any system installed inside a company and are crucial in safeguarding the business's information assets. Following the onset of the coronavirus disease 2019 (COVID-19) pandemic, some firms have offered workers the opportunity to work remotely. In cybersecurity, the responsibilities of people in protecting information assets are garnering more attention, particularly when the efficacy of security systems intended to defend firms against cyberattacks has not met expectations (Ho & Gross, 2021). company responses to a data breach may profoundly affect share value and

reputation, categorizing the incident as a cyber crisis and resulting in further long-term implications for company continuity and resilience (Wang & Park, 2017). The bulk of breaches stem from human mistake; recovering lost data is costly, and the security response often incurs substantial extra expenditures (Kang et al., 2022). Consequently, the dissemination of techniques pertaining to cybersecurity events has become a vital subject for research and implementation. It is advisable to provide education and training for workers to enhance their understanding and awareness of information security (Aldawood & Skinner, 2018). Security education, training, and awareness (SETA) programs have shown efficacy in enhancing workers' attitudes towards the adoption of suitable cybersecurity practices (Kennedy, 2016). A SETA program encompasses several subjects and may substantially enhance workers' abilities to maintain cybersecurity. This program entails instructing staff on the proper use of an organization's websites, systems, accounts, emails, and social media, while also addressing sound judgment, ethics, and the need for awareness training. Through the implementation of SETA, personnel may acquire skills to avoid and react to cybersecurity attacks and to discover vulnerabilities, therefore actively protecting the organization's data and sensitive information.

Researchers emphasize the need of management assistance to enhance workers' security awareness to requisite levels (Tsohou et al., 2009). Successful execution of the SETA program requires comprehensive assistance from top management to facilitate staff compliance with established processes (Wang et al., 2022; Tu & Yuan, 2014). An increase in support will result in more resource allocation for security-related matters (Herath & Rao, 2009). Furthermore, research indicates that personnel who have already faced a cybersecurity threat have improved attitudes towards implementing essential cybersecurity practices (Haeussinger & Kranz, 2013). Employees having prior experience in addressing cyber hazards demonstrate heightened vigilance while engaging with online platforms (Haeussinger & Kranz, 2013). This research aimed to evaluate workers' cybersecurity attitudes based on their job experience and prior exposure to cybersecurity risks.

Literature Review

Cybersecurity threats have emerged as a major issue for businesses due to the rapid pace of technological advancement. In order to carry out and oversee their daily operations, many companies nowadays rely on digital technology that can be accessed online. Consequently, addressing the cybersecurity behaviors of all workers in the firm is vital when building a cybersecurity strategy, which is an integral aspect of corporate strategic planning.

"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) goes the definition of cybersecurity. Restoring electronic information and communication systems, as well as preventing their loss, unlawful use, or exploitation, are all part of cybersecurity (Perwej et al., 2021). According to Tyagi (2019), cybersecurity protects data, software, and hardware associated with internet-connected systems against cyberattacks.

During this time, companies use physical and cybersecurity safeguards to stop unauthorized individuals from getting into their records and computer systems (de Gusmão et al., 2018). Because of the high monetary and sensitive value of an organization's information assets, it is imperative that these assets be protected from prying eyes. Workers can help keep sensitive information safe from prying eyes by being conscientious about how they use technology and by following best practices for cybersecurity, whether they're at the office or on the go (Gillam & Foster, 2020).

The phrase "cyber security threat" refers to any kind of hostile action that compromises the security of data or disrupts the functioning of the digital ecosystem; this includes attacks against persons, organizations, or other entities (Ghelani, 2022). In order to interrupt digital processes or compromise data integrity, these

threats may take several forms, including as denial-of-service assaults, phishing scams, and data breaches (Chang & Coppel, 2020). Cybercriminals generally launch these assaults with the goal of financial gain, but they often also attempt to cause damage to their targets, making them hostile acts with the purpose of creating disruptions (Sudhakar & Kumar et al., 2020). Concerns about cybercrime have the potential to affect company productivity. Due in large part to the quick development of new technology, the sophistication and frequency of assaults have grown over the years. Regrettably, cybercriminals are well-versed in these technologies and know how to exploit digital systems' weaknesses (Perwej et al., 2021).

The crime triangle, proposed by Dhanjani et al. (2009), states that in order for cybercrime to occur, three things must be in place: a victim, a motivation, and an opportunity. The victim is the one who is going to be assaulted. The chance to commit a crime will present itself at a certain moment, and the reason why will be its incentive. Whatever may harm, remove, or negatively effect an item or objects of interest by taking advantage of a gap in an organization's security system is considered a cybercrime or cyber hazard. The fact that technology alone cannot safeguard an organization's infrastructure is becoming more apparent by the day. Staying vigilant and establishing systems to control and track cyber risks are critical for companies. Therefore, it is essential that workers do their part to safeguard the company's data.

The literature on information security provides a detailed taxonomy of potential dangers. The origins, perpetrators, purpose, and outcomes were the four parts that Guo (2013) used to classify information security risks. Data breaches may originate from within or outside the company, have either malicious or accidental goals, and result in a variety of negative outcomes, such as the exposure, alteration, destruction, or denial of service of data. Intentional dangers include actions such as computer fraud, embezzlement, and theft, whereas inadvertent threats include things like natural catastrophes and human mistakes (such as workers entering incorrect data or accidentally deleting or modifying data). A new way of classifying risks to data protection was proposed by Narayana Samy et al. (2010):

- 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)

When issues arise with the company's technology, they are often easily handled. Nevertheless, human error is a complicated issue that may be difficult to control if not closely observed (Gillam & Foster, 2020; da Veiga et al., 2020).

Worryingly, insiders are often directly or indirectly assisting hackers get knowledge about the target firm in many of the many cyberattacks that occur daily. An organization's own workers are often the perpetrators or enablers of cyberattacks, depending on the situation (Perwej et al., 2021). An inside party's creation or facilitation of a security crisis is notoriously difficult to avoid, and insider assaults are notoriously harder to detect than those of an external hacker.

Kennedy, 2016; Flores & Ekstedt, 2015; Corallo et al., 2020). This is because workers are in a prime position to do so due to their familiarity with the company's inner workings, their legal and, often, privileged access to information and facilities, and their awareness of the whereabouts of any valuable or critical assets. According to van der Kleij et al. (2022), malicious internal threats are perpetrated by workers with the goal of exacting retribution or seeking financial benefit, whereas non-malicious internal threats are employees' accidental mistakes. Internal risks, such as data theft or information destruction, may cause security difficulties, although many businesses don't realize this.

Gillam and Foster (2020) state that organizations should prioritize investing in human capital above technology when it comes to information security. Workers who implement new technologies for the company won't know how to keep sensitive data safe

unless they have sufficient education and training on the subject (da Veiga et al., 2020).

Although certain cyber threats may not completely halt operations, they are inconvenient and have a negative impact on corporate efficiency (Funk, 2022). When it comes to improving company performance, commercial information assets are priceless, and security mishaps may be very costly. Loss of data may seem to be the sole short-term expense, but there may be much greater repercussions in the long run. Some companies just see a little bump in their total IT expenditure as a result of the damage, while others suffer significant losses in both money and goodwill. If everything goes wrong, the company would have to close its doors and all of its assets will be gone. Since the cost of protection is more than the cost of a security breach, it is beneficial to be able to minimize risk and avoid the uncertain route of recovery. According to Malik et al. (2022), security events may cause practical and legal problems. These incidents include data loss, integrity and availability issues, and confidentiality breaches. As a result, companies should not ignore the cybersecurity danger and should instead work to educate their staff.

Personal Beliefs and Professional Background in Cybersecurity

This research defines "cyber attitude" as the degree to which workers believe that following established cybersecurity protocols and being generally cautious would keep sensitive information safe. The best way to develop life experience is to take part in or at least be exposed to new things. Organizational leadership may provide formal and informal learning opportunities for employees to improve their attitude, competence, knowledge, and skills, all of which are correlated with work experience (Shaikh & Siponen, 2023; Hadlington, 2018). According to Hwang et al. (2019), workers' perceptions of their personal safety on the job correlate with their level of security awareness. Both direct and indirect exposure to security measures in the workplace contribute to a heightened state of security awareness. A person's level of awareness is determined by their ability to pay attention to both the immediate environmental cues and the broader context in which those cues are operating (Hwang et al., 2019). Consequently, workers' perceptions of cybersecurity policy compliance are positively impacted by their familiarity with security awareness and their experiences with both current and past security initiatives.

A key factor in lowering security incidents, according to the research published here, is the working experience of workers with the information systems (IS) that the company has deployed to handle business data. This includes having been on the scene of an event involving information security, having received training in the subject, and being aware of the repercussions of failing to adhere to information security standards.

The need to safeguard company information and data must be communicated to all personnel (Ani & He, 2018). On top of everything else they do for a living, they must make good use of the security measures put in place, anticipate potential dangers, and understand the consumer value of protecting sensitive information from unauthorized access. Experienced workers often know why security issues are becoming worse because of their excellent learning capacity (Szczepaniuk & Szczepaniuk, 2022). According to Wong et al. (2022), an organization's resilience may be enhanced by having more experienced personnel who demonstrate excellent practice. Information security training is necessary to help those with less experience with cybersecurity understand the gravity of the situation.

Workers with prior experience are also more likely to follow the company's security requirements and keep up with technological developments, such as the frequent introduction of new, advanced security solutions. Employees with a great deal of expertise should be enthusiastic about cybersecurity and should take great care to implement good security measures. When it comes to carrying out their professional duties or handling security risks, they may not need as much technical assistance due to their high absorption capacity and extensive knowledge of the organization's information

systems. The following theory is put out by this research in light of the above:

Working experience is a key predictor of cybersecurity attitudes among workers.

Experience with Cyber Threats and Cybersecurity Attitude

A company's personnel are its first line of protection (Ho & Gross, 2021). Failure to react in a cybersecurity-aware way by workers puts the firm at risk. Information security concerns are something that every employee should be aware of, along with the consequences that might affect the company and its workers individually (Ani & He, 2018).

In addition, workers need threat awareness training to change their actions and behaviors in response to information security threats (Ameen et al., 2021). Employees' lack of awareness regarding the organization's susceptibility to cyber-attacks or their inability to identify signs of attempted unauthorized access to data or systems can lead to security issues, according to previous research (Corallo et al., 2022; da Veiga et al., 2020).

Aside from factors like culture and personality, workers' cybersecurity attitude is impacted by their understanding of information security. Raising people's level of cybersecurity awareness relies heavily on their cybersecurity mindset (Khando et al., 2021). Some research (e.g., Pósa and Grossklags, 2022) suggests a link between the formation of robust security practices and early, formal, education-related security experiences that build on behaviors shown in early childhood and long stints of full-time employment. Without enough training and exposure to cybersecurity risks, it is very difficult to secure organizational systems against the many ways attackers try to steal data. From this, the following theory was developed:

H2: Employees' perspectives on cybersecurity vary greatly depending on the severity of the threats they have faced.

Study Procedure

This study's participants were categorized into four categories based on their length of service: (1) less than one year, (2) one to five years, (3) six to ten years, and (4) more than ten years. We found that workers with more than 10 years of service were considered highly experienced users, whilst those with fewer than 10 years were considered less experienced users, based on the duration of their employment with the organization. The less seasoned workers were called "newborn babies" since they need constant reassurance from upper management in order to grasp the system's surroundings rapidly. The capability to adapt to the rate of innovation (absorptive capacity) and comprehend the implicit aspects of security dangers were both acknowledged as strengths of highly experienced staff. Also, seasoned workers were supposed to have the kind of optimistic outlook on cybersecurity that's necessary for dealing with changes like tool upgrades. To effectively safeguard information assets, one needs both absorptive capability and a cybersecurity mindset.

Workers from a variety of industries in Malaysia's Klang Valley region were the intended participants in this survey. Researchers employed purposive sampling to find participants who would be a good fit for the research. Researchers are able to choose a sample that is statistically valid for the whole population by using this sampling strategy. To determine the minimal sample size, the GPower program was used. Due to the modest impact size (0.15) and the power needed at 0.95, a minimum sample size of 119 was necessary for this research, which only focused on three variables: cybersecurity attitude, cybersecurity threat experience, and working experience. Nonetheless, 245 people filled out the survey that was both online and handed to them in person. In order to conduct the online survey, we used SurveyMonkey, which can be found at https://www.surveymonkey.com/. We then posted the URL link on social media channels like Facebook and WhatsApp. We modified the questions from Hadlington (2017) to assess cybersecurity mindset.

While the original items had already undergone validation, they were somewhat adjusted for this research. Saunders et al. (2019) state that using a well-known instrument allows for easier comparisons with other studies. Furthermore, researchers may save time and effort by using

an existing instrument instead of developing a new one (Sekaran & Bougie., 2016).

For each topic, respondents used a 5-point Likert scale, from (1) very disagree to (5) very agree. An informed consent form and a declaration of confidentiality were incorporated to address ethical concerns. First, we used IBM SPSS Statistics (Version 26) to clean the data and check for normalcy. Then, we analyzed the respondent characteristics. The research aimed to determine if there were any variations in cybersecurity attitude according to the respondent's degree of job experience and their exposure to cybersecurity threats. A one-way analysis of variance (ANOVA) and an independent t-test were administered using Excel. The results are detailed in the section that follows.

Results of the Study

Personal Information of Respondents

For this study's final analysis, 245 data sets were obtained from the intended respondents. Table 1 shows that, according to the demographic information, there were more female responses (55.9%) than male (44.1%). Only 33 people, or 13.5% of the total, were older than 40 years old, while 86.5% were younger than that age. Among the industries represented, the education sector had the highest percentage of responders (23.7%), followed by banking and finance (18.4%), and finally, transportation and automotive (11.4%). While 55.5% of respondents had a bachelor's degree or above, 22.9% held a diploma, 11% held a master's, 4.9% held a professional degree, and 1.6% had just attended elementary and secondary school.

Regarding occupational status, 26.1% of respondents were managers and 30.6% were executives. Academicians (23.7%), low-level posts (3.7%), and others (15.9%) were the other occupations chosen. Among those who took the survey, 60% had less than ten years of job experience, while 40% had ten years or more. Table 2 shows that 68% of respondents had dealt with cybersecurity concerns, whereas 38% had never been the target of a cyberattack. The respondent's profile information is included in Tables 1 and 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

The normality of the data was tested by measuring skewness and kurtosis. The cybersecurity attitude skewness score was 0.238. This proved that the data set was somewhat symmetrical and favorably biased. Cybersecurity attitude has a kurtosis score of 0.840, which is below 3. According to Evans (2017), this meant that there was a lot of dispersion and the sample data curve was flat. Table 3 contains the specifics of the descriptive analysis findings.

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

There were 10 measures measuring cybersecurity attitude; for each, we found the average (mean) and standard deviation. All items had mean scores higher than 3.0, with the exception of two items that were quite near to 3: item 7 (mean value = 2.947) and item 9 (mean value = 2.976). In question 7, we inquired as to whether or not the responder was concerned that the company's image may be harmed if they went to the authorities about a hack. This assertion was disputed by the vast majority of responders. Item 9 meanwhile inquired as to whether or not the worker is unaware of how to notify a cyberattack. The majority of respondents understood what cyberattacks were and how to report them when they happened at their company, according to the mean. In addition, a large portion of the participants understood their part in preventing cybercrime at work. This proved that the responding groups had done their part and put a SETA into action. The bulk of the respondents' data is near to the mean value, according to the standard deviation statistics. In Table 4 you may see the aggregate outcomes of descriptive analytics.

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

Low (mean value from 1.0 to 2.6), Moderate (mean value from 2.7 to 3.6), and High (mean value from 3.7 to 5.0) were the three categories into which cybersecurity attitude scores were categorized in this research. Table 5 displays the descriptive-analytical results, which show that most workers have a high or moderate degree of cybersecurity attitude, with just three employees falling into the poor category.

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

This research was based on the testing of two hypotheses. One looked at the average

cybersecurity attitude of workers with varying levels of expertise on the job to see whether there were any noticeable variances or similarities. One to five years, six to ten years, and more than ten years of work experience were the four categories assessed. To test Hypothesis 1 (H1), we employed one-way ANOVA (see to Table 6 for details). Table 6 shows that the results of the analysis of variance reveal that the f-value (417.647) is higher than the Fcrit value (3.861). While this was going on, the p-value was less than 0.05, coming in at 0.00. So, we may accept Hypothesis 1 (H1) and say that there was a substantial difference in the cybersecurity mindset of workers depending on their working experience.

Table 6: One-Way ANOVA Analysis Result

Hypothesis	Variables	Average	Variance	f	p	Fcrit
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.

Additionally, cybersecurity threat experience was used to examine the difference in cybersecurity attitudes across the personnel. Two groups of respondents were formed based on their level of familiarity with cybersecurity threats: those who had experience with such threats and those who had not. In a two-sample hypothesis test, the t-statistical value (24.415) was found to be greater than the critical value (1.651), as shown in Table 7. In the meanwhile, the p-value was less than 0.05, coming in at 0.00. Based on their level of exposure to cybersecurity threats, workers' perspectives on the topic varied significantly. Accordingly, we accept Hypothesis 2 (H2).

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

To protect businesses in today's tech-driven world from cyber threats, cybersecurity is more important than ever. Accordingly, the overall security condition in the firm is highly dependent on employee attitudes towards cybersecurity (Hadlington, 2018). The study's findings show that workers' perspectives on cybersecurity differ greatly depending on their level of expertise in the field. Kennison et al. (2021) found that experienced workers often have a greater grasp of cybersecurity due to their exposure to security techniques. This conclusion is in agreement with that. In addition, facing risks like phishing might encourage workers to be more cautious while using the internet. These individuals will most likely adhere to standard procedures and rules regarding cybersecurity.

Employee morale might take a nosedive when they face cybersecurity risks head-on. Cyberattack survivors may have a heightened awareness of the risks (Alanazi et al., 2022). A cautious and proactive attitude to cybersecurity

might be inspired by these interactions. They have seen the industry evolve, therefore those with more experience usually know what they're doing when it comes to basics of cybersecurity. Staff members without experience, meantime, could be technically competent but negligent when it comes to identifying and mitigating risks.

Conclusion

Because they do not have enough information or because accessing the information is onerous, organizations may believe that supplying security information is not important for their organization. The purpose of the research presented here was to show how an organization's cybersecurity mindset affects its operations. The present research shows that the cybersecurity culture of a business is shaped by the attitudes of its employees, and that seasoned workers may set a good example by doing what they preach. A culture of security awareness and accountability may be fostered when more seasoned employees teach their less experienced colleagues.

Overall security efficacy is directly linked to the strength of the cybersecurity culture. In order to enhance the cybersecurity attitudes of workers, Corallo et al. (2022) propose that the firm establish a SETA program. Employees' attitudes about engaging in appropriate cybersecurity protective behavior may be improved by this sort of training, which is significant. Regardless of one's position within the company, all workers should be required to attend the SETA at its annualization. Employees may be asked to take part in hands-on activities throughout the program to ensure they fully grasp the processes and can effectively apply them. Highlighting what an employee should do in the event of a data breach helps decrease the likelihood of such incidents, and the exercises aid in the development of problem-solving abilities (Szczepaniuk & Szczepaniuk, 2022).

Data security education is critical because it lessens the likelihood that threats to the company, such ransomware and email phishing, which are both connected to human mistake, will succeed. Testing workers on what they've learned in training is another recommendation. Furthermore, it is critical to collect their input in order to help the business enhance and future-proof the training program (Alanazi et al., 2022). Research shows that raising security knowledge may affect workers' mindsets, which in turn improves their security behavior. It is possible to penalize workers who knowingly seek to misuse or abuse company information (Hadlington, 2017). The best strategy to deal with this problem is a well-functioning SETA program.

To ensure effective cybersecurity, it is necessary to have a monitoring system to detect policy breaches and appropriate controls to maintain a basic level of security information security training is a must for all staff members so that they may learn the ropes and understand how to properly handle, store, and delete sensitive information. In order to protect themselves against cyberattacks and data breaches, businesses should provide their staff with the knowledge, understanding, and skills to do their part. Therefore, it is crucial for management to educate and train staff on information security and properly execute security awareness programs or campaigns to ensure that all employees have enough expertise in this area.

Employees, particularly those handling sensitive information, should be involved in security strategic planning so they can learn about the organization's overall security strategy and why it's crucial to stay vigilant against new cyber threats.

It is the collective responsibility of every employee to keep sensitive company data safe. Establishing security standards and keeping personnel informed of current threats and plans are responsibilities that fall squarely on the shoulders of senior management. People, especially average individuals may not have extensive computer understanding and, without proper training, might cause damage to an organization's data system or information. As a result, SETA programs will provide a structured and efficient means of teaching, training, and bringing attention to the need of data security. Consequently, security incidents may reduce as a consequence of increased security awareness among personnel. Organizational data and user

information might be more safeguarded in this way.

The organization's regular operations might be interrupted if data breaches and illegal access to critical information are not treated carefully. Not only does information security ensure the safety of data, but it also has many other positive effects on the firm, its customers, and workers. Without it, things like business continuity would be in jeopardy. Threats from both within and outside the organization may be lessened with solid information security measures. Those in charge should make sure that everyone who uses the company's systems, whether they work for the company or not, knows how to keep sensitive information safe.

Training and awareness initiatives assist with this. Unfortunately, not all businesses are persuaded that this is the best approach to address information security concerns, thus they do not execute such programs often enough. Information security should also get funding. A key factor in encouraging staff to adopt and maintain the security measures is clear leadership backing. Data security and the repercussions of data breaches on the organization must be continually emphasized via training and awareness campaigns.

It is critical that everyone understand the importance of information security. There are a number of approaches to this, some of which are expensive. It may be easier to raise awareness of information security among system users if more conventional and digital approaches were used together; for example, a combination of video, ads, newsletters, and posters. To keep sensitive company data safe, a firewall isn't adequate. Because firewalls aren't perfect and can't keep up with dynamic threats, this is the case. Because firewalls are still controlled and designed by humans, they are not inherently intelligent and may be impacted by human error on occasion. Expertise is necessary for firewall setup and administration.

Finally, information security problems should not be ignored by any organization, no matter how big or little. This is where the organization may begin adopting security measures if they have not already. Further, biometrics, virtual private networks, and anti-malware software may all be used to handle technical elements of security. It is important to set aside funds specifically for the technology that will be employed in order to keep the maintenance contracts under budget. Organizations as a whole may be able to avoid more severe information security breaches if they combine their efforts.

References

1. 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
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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.
11. 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.
12. 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/
13. 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
14. George, D., & Mallery, P. (2003). SPSS for Windows Step by Step: A Simple Guide and Reference. 11.0 update (4th ed.). Allyn & Bacon.
15. 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
16. 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.
17. 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
18. 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.heliyon2017.e00346
19. 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
20. 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
21. 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
22. 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
23. Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security awareness: The first step in information security compliance behavior. Journalof Computer Information Systems, 61(4), 345–356. https://doi.org/10.1080/08874417.2019.1650676
24. 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
25. 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
26. 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
27. Kennison, S. M., Jones, I. T., Spooner, V. H., & Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails.
28. Computers in Human Behavior Reports, 4, 100132. https://doi.org/10.1016/j.chbr.2021.100132
29. 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
30. 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
31. 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
32. 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
33. 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
34. 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.
35. 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
36. 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
37. 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
38. 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
39. 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

40. 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
41. 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
42. 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
43. 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.
44. 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