ABSTRACT

Objective: Cybersecurity threats are a growing concern around the world. Research found that the weakest element in the cybersecurity chain is that of the human. The use of security technologies failed to address the problem in instances where employees engage in activities that place themselves and the company at risk. Hence, the role human factors play in cybersecurity is crucial. The present study aims to examine the effects of information security issues awareness, top management support, leadership, information security policy and cybersecurity awareness training on risky cybersecurity behaviour among employees in water sector.

Method: The quantitative method was applied in this study. The data were collected from 425 employees from four water companies located in northern states of Malaysia. The respondents are selected using disproportionate stratified random sampling technique. The survey was conducted using questionnaire. PLS-SEM was used to test the proposed hypotheses.

Results: The results show that security issues awareness and top management support are negatively related to risky cybersecurity behaviour. This suggest that the greater security issues awareness and top management support, lower the tendency to engage in risky cybersecurity behaviour among employees. Contrary to the prediction, cybersecurity awareness training was found to be positively related with risky cybersecurity behaviour.

Conclusions: The findings of the study have several theoretical and practical implications. Security issues awareness and top management support are important factors to avoid threat of cyber-attacks. By ensuring cybersecurity, water security is stored hence the well-being of people is taken care since water is a fundamental need of human lives. The stability and security of the country also can be maintained with secure and sustainable water resiliency. Finally, the economic losses due to cyber-attacks can be reduced.

Keywords: cybersecurity, water sector, risky cybersecurity behaviour, employees.
OS DETERMINANTES DO COMPORTAMENTO DE SEGURANÇA CIBERNÉTICA ARRISCADO: UM ESTUDO DE CASO ENTRE FUNCIONÁRIOS DO SETOR DE ÁGUA NA MALÁSIA

RESUMO

Objetivo: as ameaças à segurança cibernética são uma preocupação crescente em todo o mundo. A pesquisa descobriu que o elemento mais fraco da cadeia de segurança cibernética é o humano. O uso de tecnologias de segurança não resolveu o problema nos casos em que os funcionários se envolvem em atividades que colocam a si mesmos e à empresa em risco. Portanto, o papel que os fatores humanos desempenham na segurança cibernética é crucial. O presente estudo tem como objetivo examinar os efeitos da conscientização sobre questões de segurança da informação, apoio de alta gerência, liderança, política de segurança da informação e treinamento de conscientização sobre segurança cibernética em comportamentos de risco em segurança cibernética entre os funcionários do setor de água.

Método: O método quantitativo foi aplicado neste estudo. Os dados foram coletados de 425 funcionários de quatro empresas de água localizadas nos estados do norte da Malásia. Os inquiridos são selecionados utilizando técnicas desproporcionadas de amostragem aleatória estratificada. A pesquisa foi realizada por meio de questionário. O PLS-SEM foi utilizado para testar as hipóteses propostas.

Resultados: Os resultados mostram que a conscientização sobre questões de segurança e o suporte de alta gerência estão negativamente relacionados ao comportamento arriscado de segurança cibernética. Isso sugere que quanto maior for a conscientização das questões de segurança e o suporte da alta gerência, menor será a tendência de se envolver em comportamentos arriscados de segurança cibernética entre os funcionários. Contrariamente à previsão, verificou-se que a formação de sensibilização para a cibersegurança está positivamente relacionada com comportamentos de cibersegurança de risco.

Conclusões: Os resultados do estudo têm várias implicações teóricas e práticas. A conscientização sobre problemas de segurança e o suporte de gerenciamento superior são fatores importantes para evitar a ameaça de ataques cibernéticos. Ao garantir a cibersegurança, a segurança da água é armazenada, e o bem-estar das pessoas é assegurado, uma vez que a água é uma necessidade fundamental das vidas humanas. A estabilidade e a segurança do país também podem ser mantidas com uma resiliência segura e sustentável da água. Por último, as perdas econômicas resultantes de ciberataques podem ser reduzidas.

Palavras-chave: segurança cibernética, setor da água, comportamento arriscado de segurança cibernética, funcionários.

1 INTRODUCTION

With the rapid pace of globalization, digitalization, and smart technologies, cyber threat is becoming a daily struggle for businesses and government agencies. Digitalization is one of the most dynamic global trends in the 21st century, reshaping industries, economies, and societies at an unprecedented rate (Klimovskikh et al., 2023). As
organizations increasingly rely on interconnected networks and data-driven technologies, the vulnerability to cyber threats has heightened, necessitating robust cybersecurity measures and continuous adaptation to emerging risks. Cyber vulnerabilities pose significant corporate risks, such as downtime, data breaches, and financial losses (Sheehan et al., 2019). Annual global cybersecurity spending is approaching $100 billion, while global business losses due to cyber incidents are approaching $1 trillion (Wirth, 2017). In 2020, it is estimated that inadequate cybersecurity will cost the global economy USD 945 billion (Smith et al., 2020). By 2025, cyberattacks are expected to cause damages of about $USD $10.5 trillion annually, a 300 per cent increase from 2015 (Morgan, 2022).

Cyberattacks on a country's critical infrastructure can seriously damage the country's security and stability (Francis, 2018; Frank, 2022). National Cyber Security Policies (NCSP) were developed in Malaysia specifically to address cyber risks to Critical National Information Infrastructure (CNII) (Malaysia Cybersecurity Strategy 2020-2024). CNII refers to assets (both physical and virtual), systems, and operations that are so critical to a nation's economic strength, national image, national defence and security, government capability to function, and public health and safety that their incapacity or destruction would be disastrous (NASCA, 2022). National defence and security, banking and finance, information and communications, energy, transportation, water, health services, government, emergency services, and food and agriculture are among the ten critical sectors that have been identified as CNII (NASCA, 2022).

Water sector, as one of the country's critical infrastructures, plays an important role in national development and people's well-being around the world. Water operators all over the world have switched to smart water management systems to ensure sustainable water supply management. According to Technavio analysts, the global smart water management market was worth around $7 billion in 2015 and is expected to reach $16.73 billion by 2020 (Lee & Gourbesville, 2018). Smart water management have been adopted by utilities around the world, including Thames Water in the United Kingdom, which launched a 15-year programme to deploy smart metres across 3.3 million properties, and Manila Water in the Philippines, which used data-driven pressure optimization to improve services for over 6.2 million people (Rasekh et al., 2016). Germany is leading the way in the digitization of metrology, taking the lead in the
drinking water sector. It is estimated that there are at least 48 million water meters in municipal water networks in Germany (Gelsenwasser, 2021).

However, because of the use of automated monitoring and control systems which are connected to internet, such as the Supervisory Control and Data Acquisition System (SCADA), the water sector has become increasingly vulnerable to cyber-attacks. As most network devices in the infrastructure are frequently accessible to the public and lack sophisticated security features, it is thus an easy target for attackers (Fiza, 2022). Among the 16 lifeline infrastructure sectors, the water and wastewater sectors (WWS) were identified as one of the primary targets for cyberattacks by the United States Department of Homeland Security (DHS) (White House, 2013). According to the Industrial Control Systems Cyber Emergency Response Teams (ICS-CERT), 25 water utilities reported cybersecurity incidents in 2015, placing WWS as the third most targeted industry in the United States (Matthew & Gloria, 2018).

In Malaysia, the water industry has gone through the restructuring exercise, under the Water Policy Reform that has been introduced in Peninsular Malaysia and the Regions Labuan Federation since 2008. It aims to improve operational performance and water operator finances (Laporan Tahunan SPAN, 2020). As part of the restructuring exercise, water operators have invested in upgrading their services and facilities. Currently, water industry in Malaysia is set to migrate into smart water management. States like Selangor and Penang is leading the initiative. Selangor for example used various IoT technologies and has set up the Intelligent Command Centre and Data Analytics Centre. They also had installed Smart Meter, Automatic Chlorination Secondary System, Unit Catchment and Waterway (Air Selangor, 2021). Although there are no incidents of cyber-attacks reported in water sector in Malaysia, however, given the current development in water sector which has taken initiatives to migrate to smart water management, Malaysia too exposed to cyber-attacks. As the country embarking on the smart water management, it is imperative to remain vigilant toward possible cyber-attacks in this sector.

Several academics have commented that, for the most part, human is the weakest link in the cybersecurity chain (Anwar et al., 2016; De Bruijn & Janssen, 2017). Human mistake is responsible for 99% of successful assaults (Othman, 2018). Security technology that has been installed has failed to solve the issue when workers fail to follow cybersecurity standards or participate in actions that endanger themselves and the firm. The increasing complexity of cyberinfrastructure, the interdependence of its components,
and human behaviour has escalated the cybersecurity threats (Lange et al., 2016; Hadlington, 2018). However, research focusing on human elements has concentrated on the human-factor vulnerabilities connected to technical vulnerabilities such as lack of knowledge and skill capabilities (e.g., Asgharpour et al., 2007; Goodall et al., 2009; Wang, 2013; Ani et al., 2019).

Since most cyber incidents are human-enabled, there is a dire need to expand existing research to underexplored areas such as behavioural aspects of cybersecurity (Lahcen et al., 2020). Risky cybersecurity behaviours has been identified as actions that are widely known to increase the susceptibility of personal or organizational information assets to harm. According to Aivazpour and Rao (2018), risky cybersecurity behaviours refer to engagement in behaviours that are generally known to increase the vulnerability of personal or organizational information assets. They further explained that the risky cybersecurity behaviours correspond to those acts that are listed as unsafe in compliance guidelines of organizations. Mustafo et al. (2021) argued that behavioural sciences focused on user behaviour can provide key techniques to help increase cyber security. In their study, they have identified current research on psychological factors and individual differences among computer system users that explain vulnerabilities to cyber security attacks and crimes. A deeper understanding of factors contributing to risky cybersecurity behaviours could be the key to managing an effective cybersecurity posture within an organisation in critical sectors. Therefore, the aim of this study is to examine the factors that could have effect on risky cybersecurity behaviour among the employees in the water sector in Malaysia.

2 THEORETICAL FRAMEWORK

2.1 RISKY CYBERSECURITY BEHAVIOUR

Human behaviour associated with cybersecurity threats and incidents is termed risky cybersecurity behaviour in the literature (Schaik et al., 2017). Risky cybersecurity behaviour can be described as actions that increase the vulnerability of personal or organizational information assets (Aivazpour & Rao, 2018). Such behaviour includes clicking on a phishing link (Butavicius et al., 2016) or sharing passwords with unauthorized individuals (Aivazpour & Rao, 2018). These actions can put people at risk online and increase the likelihood of a cybersecurity breach or malicious attack (Milne et al., 2009; Hadlington, 2018). Risky cybersecurity behaviours can lead to cybercrime,
which costs billions of dollars globally and is not limited by physical borders between nations. Various individual, organisational, and contextual factors have been linked to risky cybersecurity behaviour. According to Herath and Rao (2009b), corporate (organization), contextual, and individual factors influence employees' adherence to cyber security practices. Information security awareness has been identified as an important individual factor that will help individuals to remain vigilant about cyber threats and refrain from engaging in risky cybersecurity behaviour (Kayworth & Whitten, 2010; Werlinger et al., 2009; Flores & Ekstedt, 2016).

Organisational factors such as top management support posited to influence information security perceptions, beliefs, and attitudes (Hu, Hart, & Cooke, 2007). This contention is supported by Cuganesan, Steele, and Hart (2018) in their study on the influence of top management and workplace norms on information security attitudes and self-efficacy. According to Von Solms and Von Solms (2004), leadership plays a vital role in information security within organizations, and leadership must take on the responsibility of governing information security in organizations. Providing information security training and awareness to employees should help equip them with necessary information security skills and knowledge, and therefore, improve information security compliance behaviour (Siponen, Adam Mahmood, & Pahnila, 2014). Additionally, a clear information security policy at organization can also help to address the cybersecurity issue. Information security policy is a statement of intentions and directions from management to employees to prevent or mitigate risks or threats to information confidentiality, integrity, and availability (Wood, 1995).

2.2 INFORMATION SECURITY ISSUES AWARENESS AND RISKY CYBERSECURITY BEHAVIOUR

The term information security awareness refers to being mindful of and aware of information security procedures, risks, and threats (Siponen, 2000). Furthermore, information security issues awareness refers to users' understanding of the importance of information security and their responsibilities, as well as their actions to maintain adequate levels of information security control (Shaw et al., 2009). Although the importance of employee information security awareness has been widely recognised, studies show that it remains a difficult topic because most employees are unaware of security issues, policies, and procedures (Pahnila et al., 2007). Besnard and Arief (2004)
define information security awareness as users' or employees' awareness of an organization's security mission. When defining the concept of information security awareness, most authors use at least one of these dimensions: knowledge, attitude, and behaviour (Olivos, 2018).

AlMindeel and Martins (2020) suggested that organisations’ information security awareness endeavours attribute their positive impact on individual information security behaviour. Information security awareness often employed as a preventive approach which will reduce the risk of employee negligence that mitigates risks originating both internally and externally (D’Arcy et al., 2009; Bulgurcu et al., 2010; Haeussinger & Kranz, 2013). Furthermore, for an organization's information security strategy to be effective, it must be successfully implemented (Siponen, 2000; Dinev & Hu, 2007). The findings of the study proposed the need to increase the security awareness of the corporate organisation, particularly because of the vulnerabilities they are exposed to (Adu & Ajei, 2018). On one hand, increased awareness of information security issues can lead to individuals taking more proactive steps to protect their sensitive information and avoid engaging in risky behaviour. For example, if someone is aware of the dangers of phishing emails, they may be less likely to click on a suspicious link or enter personal information into a fake website. Drawing on the above arguments, we propose the following hypothesis:

H1: There is a negative relationship between information security issues awareness and risky cybersecurity behaviour

2.3 TOP MANAGEMENT SUPPORT AND RISKY CYBERSECURITY BEHAVIOUR

Top-level management must support the development of organisational structure that prioritise cybersecurity (Hu et al., 2012). Many studies in the field of knowledge management have attempted to explain the role of top management support (Abbaszadeh et al., 2010; Ghasemi & Valmohammadi, 2018; Lee et al., 2012; Lin, 2011; Lin, 2014; Migdadi, 2009; Yip & Ng, 2019). The degree to which top management understands the importance of the information security function and is personally involved in information security activities can be defined as top management support (Thompson, 1967). Raghunathan and Raghunathan (1988) verified the importance of top management support as a critical ingredient in the success of information system planning. For managerial implications, a supportive managerial attitude and environmental
nourishment would provide information system personnel with an encouraging environment in which they believe that their work will be recognized and appreciated.

Considering information security as a management and business issue, top management can be better aware of the importance of the development and implementation of information security controls. Security control implementation can be a very complicated and resource-intensive process that requires resources and expertise (Chang & Ho, 2006). Top management can be convinced of the value of information security and the role that information security management processes play in the context of the company (Smith & Jamieson, 2006; Werlinger et al., 2009). The top management has a direct corporate governance responsibility for ensuring that all the information assets of the company are secure (Von Solms & Von Solms, 2004). The relationship between top management support and risky cybersecurity behaviour is often a negative one. When top management prioritizes and supports information security within an organization, employees are more likely to take cybersecurity seriously and adopt safe practices. This can help to reduce the risk of cyberattacks and minimize the impact of any incidents that do occur. Drawing on the above arguments, we propose the following hypothesis:

H2: There is a negative relationship top management support and risky cybersecurity behaviour

2.4 LEADERSHIP AND RISKY CYBERSECURITY BEHAVIOUR

Leadership is critical to information security within organisations, and leadership must assume responsibility for governing information security within organisations (Von Solms & Von Solms, 2004). Solms and Von Solms (2004) asserted that leadership plays a vital role in information security within organizations and that leadership must take the responsibility of governing information security in organizations. Leadership refers articulating a clear vision about the Information Security Policy (ISP), formulate a clear strategy for achieving effective ISP, establishing clear goals/objectives for attaining effective ISP to protect the organization’s assets against threats (Hu et al., 2012; Paliszkiewicz, 2019). Tubbs and Schulz (2006) define leadership as the individuals that influence others in order to achieve the goals of the organization. Hu et al. (2012) found that leadership significantly influenced employees’ behaviour and their intention to comply with information security policies.
According to Triplett (2022), one way of creating accountability is by creating a cybersecurity charter, signed by cybersecurity leadership and other members of the company’s executive leadership, in which all leaders agree to not expose the organization to risk. Furthermore, organizations need to implement leadership development programs to better prepare their cybersecurity leaders to work with other employees. Developing cybersecurity leaders is an investment, and the return on this investment will take the form of reduced cybersecurity risk (Rotherberger, 2016). Leadership can play a crucial role in setting the tone for information security within an organization. Leaders who prioritize information security and emphasize its importance to the success of the business can encourage employees to take their cybersecurity responsibilities seriously and adopt safe practices. Leaders who provide the resources and support necessary for information security, such as training, technology, and a secure work environment, can also help to reduce the risk of cyberattacks. Drawing on the above arguments, we propose the following hypothesis:

H3: There is a negative relationship leadership and risky cybersecurity behaviour.

2.5 CYBERSECURITY AWARENESS TRAINING AND RISKY CYBERSECURITY BEHAVIOUR

Cybersecurity awareness training is a formal programme that teaches users about potential threats to an organization's information and how to avoid situations that could jeopardize the organization's data (Gardner, 2014). Cybersecurity training is both formal and informal education about the risks associated with information technology. It is formal in the sense that people must attend specific training sessions (Sullivan, 2019). It is also informal because, in addition to these mandatory training sessions, there is a constant emphasis on cybersecurity at senior staff meetings, through the employee review process, and through frequent reminders about the daily responsibilities associated with cybersecurity vigilance (Sullivan, 2019). Cybersecurity training can also help information system users gain a better understanding of security and data protection methods, resources, and policies. Cybersecurity training can also help users of information system deepen their understanding of security and data protection methods, resources, and processes for using computers, software, and online applications (Indeed Editorial Team, 2021). Crafting person-organization fit through organizational interventions such as cybersecurity training will be able to promote organizational citizenship behaviour among...
employees in the form of compliance to cyber behaviour (Sabrina, Harahap, Datuk, 2023).

Disparate and Furlow (2017) suggest that the best cybersecurity investment that an organization can make is stronger security training for its employees. That is why organizations must invest in cybersecurity awareness training (CSAT) to increase their employees’ awareness and readiness (Schmidt et al., 2008; He et al., 2019). Zhang et al. (2021) explored different types of CSAT programs and their impact and implementation. By weighing the trade-offs between their desired level of security and the overall cost of achieving it, businesses can create their ideal cybersecurity strategy (Pigni, 2019). Through training, employees can learn about the latest information security threats, such as phishing scams, malware, and data breaches. They can also learn about best practices for protecting sensitive information and reducing the risk of cyberattacks. When employees receive regular and effective cybersecurity awareness training, they are more likely to take their information security responsibilities seriously and adopt safe practices. Drawing on the above arguments, we propose the following hypothesis:

H4: There is a negative relationship between cybersecurity awareness training and risky cybersecurity behaviour

2.6 INFORMATION SECURITY POLICY AND RISKY CYBERSECURITY BEHAVIOUR

Information security policy (ISP) is a set of instructions that define what users should do and should not do, pointing out reasonable behaviour to secure the information and information assets (Hone & Eloff, 2002). To achieve ISP objectives, a robust security framework must ensure the confidentiality, integrity, availability, authenticity, authority, verifiability, and nonrepudiation of critical information assets (Alhanahnah et al., 2016). ISP is a governing document that defines the overall boundaries of information security in an organisation (Sohrabi et al., 2016; Lucila, 2016). It also demonstrates management’s commitment to and support for information security in an organisation and the role it plays in achieving and supporting the organisation’s vision and purpose (Sohrabi et al., 2016; Knapp et al., 2009; Kadam, 2007; Lucila, 2016).

According to Li et al. (2014) employees in an organization that has an explicit security policy in place tend to be more worried about security breaches if they don’t adhere to the company’s information security policy and are more responsible for taking
appropriate measures to protect cybersecurity of their organization. Information security policies are significant for consideration in different organizations since they help businesses to identify best practices and methods for use to be equipped against cyber threats and the loss of valuable data (Taherdoost et al., 2015; Taherdoost et al., 2020). The main aim of information security policy is to prevent or mitigate cyberattacks and reduce the risk of cyber threats (Purser, 2014). When an organization implements a comprehensive information security policy, it sets clear expectations for employees regarding their responsibilities for protecting sensitive information. An information security policy should outline the specific practices and procedures that employees are expected to follow, such as using strong passwords, regularly updating software, and reporting any suspicious activity. When employees are aware of these policies and understand the consequences of not following them, they are less likely to engage in risky behavior. Drawing on the above arguments, we propose the following hypothesis:

H5: There is a negative relationship between information security policy and risky cybersecurity behaviour

2.7 RESEARCH MODEL

Figure 1 presents the proposed model for the current study with the main objective to examine the factors that could influence risky cybersecurity behaviour. The dependent variable of this study is risky cybersecurity behaviour while the independent variables consist of information security issues awareness, top management support, leadership, cybersecurity awareness training, and information security policy.
3 METHODOLOGY

3.1 POPULATION, SAMPLE AND SAMPLING TECHNIQUE

In this study, the total population is 4,154 employees working in water companies in northern states of Malaysia consist of Perlis, Kedah, Penang, and Perak. This study, however surveyed 425 respondents selected using disproportionate stratified random sampling technique. Disproportionate stratified random sampling is deemed appropriate option since the number of members (employees) in each stratum (states) is not balance. The respondents come from a variety of departments, ages, and positions, among other things as long as they fit the inclusion criteria set for the research.

3.2 DATA COLLECTION PROCEDURES

Suruhanjaya Pengurusan Air Negara (SPAN), who is the water regulator in the country was first contacted to obtain the letter of recommendation before the water companies are approached. The letter of support from the above central agencies was very helpful to get positive response and cooperation from the participating companies. Secondly, the researchers contacted the corporate communication or human resources department of the water companies to obtain the data about the total number of employees and permission to conduct the survey. Thirdly, once all parties have agreed, the researchers visited each water industry company and hand out the questionnaires based on the number of respondents identified for each company. Fourthly, during the given time frame, the researcher did the follow up with the person in charge at respective participating companies. Lastly, the researchers return to each company to collect the questionnaires that have been answered.

3.3 QUESTIONNAIRE TRANSLATION AND PRE-TEST

Although the original instrument is in the English language, the questionnaire was prepared in the Malay language to allow respondents to answer in the language that they are familiar with. Back translation was employed in that the original instrument was translated into the Malay language by academic experts in both languages. The translated version was later back translated into the English language to confirm the match between the original and the English translated version by a different group of academics. This back translation process followed the procedure suggested by Brislin (1970).
was conducted to assess the face validity, and very minor changes were incorporated into the final questionnaire.

3.4 MEASURES

Information security issue awareness refers to users' understanding of the importance of information security and their responsibilities and actions to maintain adequate levels of information security control (Shaw et al., 2009). The information security issues awareness consist of three questions adapted from Koohang et al. (2019). A sample item is, “Overall, I am aware of potential security threats and their negative consequences”. The internal consistencies (Cronbach’s alpha) of the scale was 0.925 in a previous study conducted by Koohang et al. (2019).

Top management support was measured with the 6-item adapted from Knapp et al. (2006). Top management support defined as the degree to which top management understands the importance of the IS function and is personally involved in IS activities (Thompson, 1967). Respondents were asked to use a seven-point Likert-type scale, ranging from 1 (strongly disagree) to 7 (strongly agree) to rate the items. A sample item is, “Senior management considers information security an important organizational priority”. The scale was reported to have a Cronbach’s alpha of 0.944 in a study conducted by Tenzin (2021).

Leadership refers to articulating a clear vision about the Information Security Policy (ISP), formulate a clear strategy for achieving effective ISP, establishing clear goals/objectives for attaining effective ISP to protect the organization’s assets against threats (Hu et al., 2012; Paliszkiewicz, 2019). The construct was measured with the 3-item adapted from Hu et al. (2012) and modified from Paliszkiewicz (2019). A sample item is, “Leadership in my organization has articulated a clear vision about ISP to protect organization’s assets against threats”. Respondents were asked to use a seven-point Likert-type scale, ranging from 1 (strongly disagree) to 7 (strongly agree) to rate the items. The scale was reported to have a Cronbach’s alpha of 0.900 in a study conducted by Bagozzi and Yi (1988).

Three items were used to measure information security policy and the scale was adapted from D’Arcy, Hovav, and Galletta (2009). The construct is to a declaration of intentions and orders from management to employees to prevent or reduce risks or threats to information confidentiality, integrity, and availability (Tenzin et al., 2021). A seven-
point Likert-type scale with rating options from 1 (strongly disagree) to 7 (strongly agree) was used to measure the construct. A sample item is, “My organization has established rules of behaviour for use of computer resources”. The items reported to have Cronbach’s alpha ranging from 0.872 in previous studies (Tenzin, 2021).

Cybersecurity awareness training was measured using six items cybersecurity awareness training instrument adapted from Knapp (2005). The construct is known as a formal program with the goal of training users of the potential threats to an organization's information and how to avoid situations that might put the organization's data at risk (Gardner, 2014). Respondents were asked to use a seven-point Likert-type scale, ranging from 1 (strongly disagree) to 7 (strongly agree) to rate the items. A sample item is, “Necessary efforts are made to educate employees about new security policies”. Tenzin (2021) reported a Cronbach’s alpha of 0.902 for the scale in their study.

4 RESULTS AND DISCUSSION

4.1 DEMOGRAPHIC PROFILE OF THE RESPONDENTS

The distribution of respondents’ location reveals that that majority of the respondents are from Perak state consist of 42.6%. This is followed by those from Kedah with 39.8%. Respondents from Penang is the third largest with 15.8%, and the least is from Perlis that comprise of 1.9%. Male respondents have more response rate with 56.7% while female are 43.3%. Majority of the respondents are in the age range between 41-50 (61.0 %). Second highest are those in range 31-40 years (44.7%), while 28.2% are within the age of 21-30 years. 10.6% includes in the age more than 50 years and 0.5% are belonging to the age range of 21 years below. Those with SPM/SPTM constituted 89 respondents which represent 20.9% of the total respondents, while, BSc degree education constituted 148 responses, representing 34.8% of the responses, Master degree education constituted 13 responses, representing 3.1% of the respondents and finally followed by professional certificates with 175 responses, representing 41.2%. The majority of respondents are Malays, consist of 396 employees or 93.2%. Indians are second largest comprises of 4.2% workers, while Chinese represented by 1.4%. Majority of the respondents worked more than 10 years (42.1%), followed by 5-10 years range (34.8%). Respondents with less than 5 years’ experience consist of 23.1%. The result also shows that 7.0% of the respondents are engineers, machine operators (0.5%), managers (4.0%), supervisors (12.0%), technicians (20.5%) and other job categories are 56.0%.
4.2 HYPOTHESIS TESTING

PLS-SEM was used to test the proposed hypotheses in this study. The causal predictive-based PLS-SEM was preferred over the confirmatory-based (CB)-SEM because of its relevancy to address the objective of this study, i.e., to examine the proposed hypotheses that are grounded in causal explanations (Jöreskog & Wold, 1982). Subsequently, SmartPLS 3.3.2 (Ringle et al., 2015) was used to estimate the model parameters (Sarstedt & Cheah, 2019).

4.3 MEASUREMENT MODEL ASSESSMENT

The measurement model assesses the relationship between the observed variables (indicators) and the latent variables (constructs) (Ramayah et al., 2018). In a reflective measurement model, three criteria of reliability and validity are assessed, namely internal consistency, convergent validity, and discriminant validity (Cheah et al., 2018). As shown in Table 1, the observed variables demonstrate good internal consistency and convergent validity on its respective latent variable. The internal consistency, measured by the composite reliability, is above the threshold value of 0.7 (Hair et al., 2017), and the loadings of each indicator as well as the average variance extracted (AVE) which denotes the convergent validity, are within the acceptable threshold. The AVE value of more than 0.5 suggest that convergent validity has been established (Hair et al., 2017).
Table 1: Assessment of internal consistency and convergent validity

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Items</th>
<th>Factor Loadings</th>
<th>Alpha</th>
<th>CR</th>
<th>AVE</th>
<th>R2</th>
<th>R2 Adj</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership</td>
<td>LE 1</td>
<td>0.971</td>
<td>0.956</td>
<td>0.97</td>
<td>0.915</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LE 2</td>
<td>0.956</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LE 3</td>
<td>0.943</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Management Support</td>
<td>MS 1</td>
<td>0.913</td>
<td>0.967</td>
<td>0.973</td>
<td>0.858</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS 2</td>
<td>0.922</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS 3</td>
<td>0.937</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS 4</td>
<td>0.935</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS 5</td>
<td>0.924</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MS 6</td>
<td>0.915</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info security Issues awareness</td>
<td>SA 1</td>
<td>0.928</td>
<td>0.851</td>
<td>0.905</td>
<td>0.761</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA 2</td>
<td>0.757</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA 3</td>
<td>0.921</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risky Cybersecurity Behaviours</td>
<td>RB 1</td>
<td>0.714</td>
<td>0.924</td>
<td>0.935</td>
<td>0.55</td>
<td>0.123</td>
<td>0.112</td>
</tr>
<tr>
<td></td>
<td>RB 12</td>
<td>0.769</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 13</td>
<td>0.709</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 15</td>
<td>0.874</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 16</td>
<td>0.812</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 19</td>
<td>0.807</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 2</td>
<td>0.502</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 5</td>
<td>0.787</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 6</td>
<td>0.57</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 7</td>
<td>0.661</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 8</td>
<td>0.798</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RB 9</td>
<td>0.807</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Policy</td>
<td>SP 1</td>
<td>0.846</td>
<td>0.897</td>
<td>0.929</td>
<td>0.813</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SP 2</td>
<td>0.948</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SP 3</td>
<td>0.908</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training and Awareness Campaign</td>
<td>TA 1</td>
<td>0.72</td>
<td>0.956</td>
<td>0.95</td>
<td>0.763</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TA 2</td>
<td>0.743</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TA 3</td>
<td>0.905</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TA 4</td>
<td>0.955</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TA 5</td>
<td>0.963</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TA 6</td>
<td>0.922</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Source: Author’s Own Findings)

As described by Hair et al. (2016), discriminant validity is an indication of how much a variable is distinct from others. Moreover, as mentioned in Duarte and Raposo (2010), higher discriminant validity indicates that the variable differs from others and that a distinct variable can measure a phenomenon that could not be measured by other variables. As a result, the model's external consistency was examined in relation to its discriminant validity. In this regard, the square root of AVE was used to calculate the discriminant validity for this investigation. To establish the discriminant validity, a
variable’s square root of AVE should be higher than the correlations between the latent variables. Table 2 shows the square root of AVE for each variable and illustrates a comparison between the correlation between the latent variables, information security issues awareness (SA) = 0.872; information security policy (SP) = 0.902; leadership (LE) = 0.957; top management support (MS) = 0.926; training & awareness campaign (TA) = 0.874; and Risky cybersecurity behaviours (RB) = 0.742.

<table>
<thead>
<tr>
<th>Fornell-Larcker Criterion</th>
<th>SA</th>
<th>SP</th>
<th>LE</th>
<th>RB</th>
<th>MS</th>
<th>TA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info Security Issues Awareness</td>
<td><strong>0.872</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info Security Policy</td>
<td>0.389</td>
<td><strong>0.902</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leadership</td>
<td>0.52</td>
<td>0.583</td>
<td><strong>0.957</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risky Cybersecurity Behaviours</td>
<td>-0.266</td>
<td>-0.095</td>
<td>-0.117</td>
<td><strong>0.742</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Mgt Support</td>
<td>0.476</td>
<td>0.59</td>
<td>0.829</td>
<td>-0.16</td>
<td><strong>0.926</strong></td>
<td></td>
</tr>
<tr>
<td>Training &amp; Awareness Campaign</td>
<td>0.195</td>
<td>0.521</td>
<td>0.527</td>
<td>0.113</td>
<td>0.53</td>
<td><strong>0.874</strong></td>
</tr>
</tbody>
</table>

(Source: Author’s Own Findings)

Note: The bolded numbers shown in Table 2 represent the square route of average while others represent latent variable correlations.

Table 2 demonstrates that for all variables, the AVE square roots are higher compared to the correlation between the latent variables. Hence, the model’s discriminant validity is at an acceptable level (Aremu et al., 2018). Initially, the hypothesised relationships between variables in the framework were projected based on past studies. As recommended by Hair et al. (2016), variables containing at least two items should be retained; hence the confirmatory factor analysis result led to the retention of all variables because they all have at least two items.

4.4 STRUCTURAL MODEL ASSESSMENT

The structural model (inner model) assesses the relationship between the latent variables in the hypothesized model (Ramayah et al., 2018). The proposed hypotheses were assessed by means of bootstrap re-sample technique using an iteration of 1,000 subsamples. Table 3 represents the corresponding results. As stipulated in H1, information security issues awareness has a significant negative impact on risky cybersecurity behaviours ($\beta=-0.231; t=3.665; p< 0.000$). The finding is consistent with past study that found individuals who have a high level of information security awareness are less likely to engage in risky online behaviour (Hammarstrand & Fu, 2015), such as sharing personal information, using weak passwords, and clicking on suspicious links. Similarly, another study found that individuals who are more knowledgeable about information security
issues are more likely to take steps to protect their personal information online and are less likely to fall victim to cybercrime (Deora & Chudasma, 2021). Overall, individuals who are more aware of the risks associated with online activities and are better informed about how to protect themselves are less likely to engage in risky behaviour that could compromise their personal information or lead to a cyberattack.

H2 of the study which postulates negative relationship between top management support and risky cybersecurity behaviour also supported (β= -0.225; t=2.535; p<0.012). Top management support is essential for creating a culture of cybersecurity within an organization. When top management prioritizes cybersecurity and provides the necessary resources, employees are more likely to take cybersecurity seriously and follow security policies and best practices. Top management support can also help to ensure that cybersecurity is integrated into business processes and decision-making, which can help to prevent cybersecurity incidents. Furthermore, top management provide support to employees based on current policies, objectives and needs. Thus, employees are more receptive to instructions and the problems of cybersecurity risks can be overcome immediately.

H3 that predicts negative relationship between leadership and risky behaviour however was not supported in this study (β= 0.086; t= 0.989; p> 0.05). Relationship between leadership and cybersecurity behaviour is complex and multifaceted, and there are many factors that contribute to effective leadership in the context of cybersecurity. Unlike top management, leadership can be provided by anyone at any level in the organization. The leaders who are not well trained usually lacks overall mastery of knowledge, strategic, reading of the current situation and analysis of possible cybersecurity risks compared to top management. Wherein, top management can look broadly from various angles and levels compared to the head who is in the middle only more focused on his own unit and division. This explains why there is no relationship between leadership and risky cybersecurity behavior.

H4 which states that training and awareness campaign will be negatively associated with cybersecurity behaviour was found to have positive significant relationship instead with cybersecurity behaviour (β= 0.263; t=2.691; p < 0.000). This suggests that the more training and awareness campaign attended by employee, greater the tendency to engage in cybersecurity behaviour. This could be due to overconfidence among the user. Employees who receive extensive cybersecurity awareness training may
develop overconfidence in their ability to identify and respond to security threats. This can lead to complacency and a false sense of security, which can lead to risky behaviour. Furthermore, this newfound awareness can spark their curiosity and motivate them to learn more about cybersecurity. Employees will be able to get caught up in cybercrime. Thus, curiosity can be a valuable trait in the context of cybersecurity because it drives individuals to seek out new information and to ask questions.

H5 suggests a negative relationship between information security policy, however this hypothesis was not supported ($\beta = -0.06; t = 0.627; p > 0.05$). In fact, some studies have found that the existence of an information security policy alone may not be enough to reduce risky behaviour among employees. It is possible that the existence of an information security policy can lead to a false sense of security among individuals or organizations. They may assume that because there is a policy in place, they are protected from all cybersecurity risks and may therefore engage in riskier behaviour than they would otherwise. Additionally, if the policy is too restrictive or difficult to follow, individuals may find ways to circumvent it, leading to risky behaviour. In other words, the relationship between information security policy and risky cybersecurity behaviour is complex and can depend on a variety of factors such as the effectiveness of the policy, the level of awareness and education about the policy among users, and the motivations of individuals or organizations.

<table>
<thead>
<tr>
<th>Path Coefficient</th>
<th>Beta</th>
<th>Standard error</th>
<th>t value</th>
<th>p value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info Security Issues Awareness $\rightarrow$ Risky Cybersecurity Behaviours</td>
<td>-0.231</td>
<td>0.063</td>
<td>3.665</td>
<td>0.000</td>
</tr>
<tr>
<td>Info Security Policy $\rightarrow$ Risky Cybersecurity Behaviours</td>
<td>-0.06</td>
<td>0.095</td>
<td>0.627</td>
<td>0.531</td>
</tr>
<tr>
<td>Leadership $\rightarrow$ Risky Cybersecurity Behaviours</td>
<td>0.086</td>
<td>0.087</td>
<td>0.989</td>
<td>0.323</td>
</tr>
<tr>
<td>Top Mgt Support $\rightarrow$ Risky Cybersecurity Behaviours</td>
<td>-0.225</td>
<td>0.089</td>
<td>2.535</td>
<td>0.012</td>
</tr>
<tr>
<td>Training &amp; Awareness Campaign $\rightarrow$ Risky Cybersecurity Behaviours</td>
<td>0.263</td>
<td>0.098</td>
<td>2.691</td>
<td>0.007</td>
</tr>
</tbody>
</table>

(Source: Author’s Own Findings)

5 CONCLUSION

The findings of this study further enhance our understanding about the human vulnerabilities related to risky cybersecurity behaviour that can lead to cyber-attack.
While past studies focused on technical aspects of cybersecurity to deter users from engage in cyber related incidents, this study adds to body of knowledge by suggesting that soft approaches are also can help to address risk to cybersecurity. Secondly, this study has focused on the key organizational factors that often neglected in past studies specially the role of top management support, leadership, information security policy and availability of training and awareness campaign related to cybersecurity that can help to address cybersecurity threats in the organization. Finally, this study has addressed the sectoral and contextual gap by conducting the study in the water sector. Past studies often concentrate in sectors that has heavily invested in advance cybersecurity technology such financial, manufacturing and telecommunication. The study in water sector, specifically in Malaysian context would add new knowledge in research related to human-aspects of cybersecurity.

The outcomes of this research will have few practical implications. By understanding factors contribute to the risky cybersecurity behaviour among employees in CNII sectors like water services industry, it can facilitate the relevant stakeholders such as water operators to successfully mitigate the cyber threats. As a result of this, first, it will help to ensure water security in the country by mitigating possible cyber-attacks in the water services industry. Hence, the well-being of people is taken care since water is fundamental human need of human lives. Secondly, the stability and security of the country can be maintained with secure and sustainable water resiliency. Thirdly, issues such as high non-revenue water (NRW) losses due to leaks, water theft, and payment defaulters can be addressed. Fourth, the economic losses due to cyber-attacks can be reduced. Fifth, with water security (SDG 6) in place, the country is committed in supporting UN's sustainable development goals (SDGs).

5.1 LIMITATIONS AND FUTURE RESEARCH RECOMMENDATIONS

There are several limitations in terms generalizability of research findings. Firstly, by studying factors contributing to risky cybersecurity behaviour, this study focused on the soft approaches to mitigate cybersecurity risk. The research did not include the technical (hard) aspects that can effect risky cybersecurity. Future research should be comprehensive and incorporate both the soft and hard approach in the study. Secondly, the sample limited to water industry in northern states of Malaysia, hence the findings are not generalizable to settings outside the scope of this study. Future research should
conduct a study with a more extensive sample involving other states as well to have a complete understanding about the phenomenon. Finally, this study proposed a direct relationship between various factors on risky cybersecurity behavior and did not include other enabler factors. Future research may include other mediator or moderator variables to have better understanding about the factors influence risky cybersecurity.

ACKNOWLEDGEMENTS

This research was supported by Ministry of Higher Education (MOHE) of Malaysia through Fundamental Research Grant Scheme (FRGS/1/2021/SS02/UUM/02/2).
REFERENCES


The Determinants of Risky Cybersecurity Behaviour: A Case Study Among Employees in Water Sector in Malaysia


