EFFECTIVE INFORMATION SYSTEM AND ORGANISATIONAL EFFICIENCY

Rahiman H.U., Nawaz N., Kodikal R., Hariharasudan A.*

Abstract: The present study aims to identify the effectiveness of information systems on organizational efficiency in technical and operational perspectives in the various public and private sectors. The novelty of the research focuses on data security practices, perceived severity, response efficacy, perceived usefulness and perceived behavioral control on organisational effectiveness. The survey data is gathered from 200 professionals representing public and private sectors in India and MENA countries who broadly support these outcomes. The analysis of data was generated by applying an equation model and various descriptive statistical tools using AMOS and SPSS. The study results reveal that an effective information system with comprehensive information management avoids potential cyber-attacks and enhances the organisation's performance. The study identified that repeated cyberattacks threaten the reputation of the business and its organizational operations. Therefore, creating effective awareness about risks and challenges on business operation among the workforce enhances the performance and efficiency of the organization. This empirical research has contributed significantly for organizations to emphasize suitable measures to incorporate effective information and risk mitigation plan to protect data and efficiency. The research outcome emphasized that training and awareness are mediating variables to enhance performance.

Key words: cyber security, internet of thinking, cyber risk, social engineering, India, MENA

DOI: 10.17512/pjms.2021.24.2.25

Article history:
Received August 31, 2021; *Revised* November 15, 2021*; Accepted* November 27, 2021

Introduction

Information and data security play an important role in all companies globally, as investors and external stakeholders demand to and depend on the modalities' trustfulness. Furthermore, companies have been mandated to act in accordance with government principles and criteria not to be exposed to penalties or punishment. Management experiences settled for data and information security help managers in applying operational risk management resulting in more incorporated security measures into the structure of an organization risk management. Conversely, in some organizations, high-ranking management is not performing the authorized security mandate and passes them to middle or low-ranking management levels. The participation and upkeep of the corporation board and high-ranking management can

* **Habeeb Ur Rahiman**, PhD, **Nishad Nawaz**, PhD, Kingdom University, Bahrain; **Rashmi Kodikal**, PhD, Graphic Era (Deemed to be University), India and **A. Hariharasudan**, PhD, Kalasalingam Academy of Research and Education, India
✉ corresponding author: dr.a.hariharasudhan@gmail.com
✉ h.rahiman@ku.edu.bh; n.navaz@ku.edu.bh; rashmikodikal@gmail.com

support in instituting a durable security structure for data and information security and refining the standards of security practices across the corporation to alleviate risk. However, security practices and measures are inclined to be laidback in some corporations as managers are not contained within security measures. There ought to be an all-inclusive approach to take account of business high-ranking managers in the process of security strategy improvement and employment.

The stimulating characteristic of information and data security and risk controlling is considering the matter at a higher level and supporting resources to control data and information security in the organization. Lack of awareness of the hazards of converse communal engineering threats can lead to an unsuspicious employee unveiling confidential business data or melting down sophisticated data and information security knowledge inadequate. Even though programmed systems can be applied to detect deceitful emails and websites, these systems are not entirely precise in discovering phishing attacks (Mantha & García de Soto, 2021). Technological solutions alone will not provide a line of protection against cyber threats or attacks, which abuse human defencelessness such as phishing. Consequently, it is indispensable for organizations to acquire the mechanisms to shield people from such threats and attacks besides methods for increasing the people's awareness so as not to be victims of phishing threats and attacks. Appropriate information and data security awareness is an operational way to shield against social engineering threats and attacks. The management related to unceasing information security attentiveness and awareness is necessary to endure a necessary level of information and data security attentiveness (Rajan et al., 2021; Bhatt et al., 2021; Al-Gasawneh et al., 2021).

Correspondingly, the security awareness techniques and programs ought to be enhanced with the purpose of indoctrinating strictly affirmative work practice to intensify protecting organizational resources and stop information and data security incidents. Success is based on keeping awareness of relevant and dependable messages simultaneously with keeping the delivery devices and mechanisms thought-provoking to everyone (Armenia, Angelini, Nonino, Palombi, & Schlitzer, 2021). A key challenge with security awareness techniques and programs is the absence of a copiously advanced methodology to provide them (Daengsi, Wuttidittachotti, Pornpongtechavanich, & Utakrit, 2021). Research on the providing technique of security awareness preparation determined that the conveyance of security awareness data and information is as significant as confirming that the information and data are pertinent and dependable (Anand, Medhavi, Soni, Malhotra, & Banwet, 2018). Nonetheless, Gulf countries are located in a region categorized in the bottom level for cyber edification and preparation where jaggedly the majority of businesses nonexistence the ability to care for themselves from erudite hacks (Gontar et al., 2018). On the other hand, India is finally clear the national cyber security strategy to prevent cyber-attacks against businesses. For that reason, businesses and organizations need to consider awareness susceptibilities with operative information and data security awareness platforms to accomplish a

sufficient security attitude. Information and data security awareness techniques and program with the purpose to generate a security-conscious setting by eradicating susceptibilities related to human performances is principal for safeguarding organizational resources. Many people are sensible of phishing; however, they do not use that attentiveness to their susceptibility or approaches for classifying phishing attacks (Porcedda, 2018; Sabillon, et al., 2019; Jibril et al., 2019).
Since effective adoption of information and cyber security systems is essential to prevent frequent cyberattacks, which causes huge intellectual and monitory loss for the business world. A powerful cyber security system is one of the vital infrastructures one organisaiton need to consider. Since the performance and efficiency of any industry rely upon comprehensive information systems, the world timely considers advanced technology like Artificial intelligence, Machine learning and Internet of thinking are essential for industrial operation. By considering these challenges and issues, this study is intended to investigate the impact of an effective information system on organisational efficiency amongst professionals working in various public and private companies in India and MENA region.

Literature Review

An effective data security practice in an organisation maintains systematic order and operational efficiency. Since businesses have been more dependent on knowledge to attain their ultimate goals, it is precarious to uninterruptedly improve the awareness principles related to the concept of security in all businesses and renovate an atmosphere of cultural organization. A cultural organization should be tinged with a real awareness of security measurements. There have been sufficient indication that, under the appropriate consciousness of the philosophy of safekeeping, employees can be converted into the business's sturdiest layer of defence against cyber-attacks (Nica, Potcovaru, & Hurdubei Ionescu, 2019). As a result, businesses have to fight against user consciousness susceptibilities by means of operational information and data programs. These programs assure the process of resilience awareness to accomplish an ample security position (Bin, Joint, Academy, & Emirates, n.d.). Currently, cyber-crimes are growing and becoming more complicated than before. Cybercrimes are illegitimate actions as a computer is not purposed for that reason. The computer is purposed for education, innovation, and productivity (Zauskova, Lyakina, Tretyak, & Miklencicova, 2020). Overall, cybercrimes are certain acts that are done by using a device, usually a computer and the internet. The purpose of cyber-crimes is to get an individual's identity over. Because gradual automation presents a significant part in an individual's everyday life, cyber-attacks will also increase at the same rate. There is a struggle between individual interests and technological risks (Rowland, Krulicky, & Oliinyk, 2020). Outmoded malware spasms happened at a particular position on the apparent amongst hardware apparatus, software subdivisions, and system stratum, through the current scheme erroneously (Nam, 2019). Therefore, enforcing and updating comprehensive data security practices and planning with suitable regulations and norms defines the

security measures, identifies the authorised access, describes the authorised uses, enforces the notification and procedures, which results in organisational efficiency. Considering these outcomes, the study has proposed the following two hypotheses.
H1: Effective data security practices enhance organisational efficiency.
H2: Perceived Severity and Subjective Norms enhance efficiency.
Organizations are progressively apprehensive about certifying that employees have adequate control over information technology (Aghakhani et al., 2020). The perceived control over information systems is a crucial factor in describing the behavioral and cognitive efforts that entities make to adjust to new and troublesome information system applications (Litchfield et al., 2017). Social engineering has become a serious issue that needs to be discussed (Ingalagi et al., 2021). Social engineering unambiguously causes much harm and threatens the human side exposing their data and information to many risks. The human side is the weak part of the cycle that security specialists need to fortify (Lazanyi & Lambovska, 2020). Phishing has been exposed to more and more advanced threats through which the attackers utilize hoaxed emails as well as mock-up websites to access private information (Caldwell, Nyre-Yu, & Hill, 2019). The most famous method to access emails is phishing attacks. The cyber-attackers are trying to abuse human trust and access private data and information related to websites and other users' activities. Cyber-attackers lean towards targeting the most important activities of users. Correspondingly, phishers have been progressively targeting social networking sites, e.g., Facebook and Twitter. A lot of people have enough idea about phishing; on the other hand, they do not subordinate that consciousness to their defenselessness or to approaches for recognizing phishing occurrences (M'manga et al., 2019). The perceived behavioral control can alleviate information system operators' anxiety and encourage emotions that they can promote from the newly applied system (Cao, Huang, Yu, & Huo, 2014). As a result of the possible significance of the role of perceived behavioral control, we need to well recognize its structure with regard to the information system in the workplace (Mathiesen, Marjanovic, Delavari, & Bandara, 2013). Accordingly, this article focuses on the hypothetical gaps surrounding perceived behavioral control and proposes the following hypothesis.
H3: Perceived Behavioral Control and Response Efficacy increase efficiency.
Many organizations consider that employees are the most valuable resource; meanwhile, many situations and cases opine that many of their' s weakest areas are safeguarding information systems (Mahadevan, Agbinya, & Braun, 2006). The weakest domain can turn out to be effective by generating awareness and training programs for individuals within the company (Kralj, 2010). Effective training and establishing awareness programs improve efficiency and reduce ambiguity and technical stigma amongst members (Sujith Kumar et al., 2011). Many organizations reserve sufficient funds and recourses to empower manpower to enhance their efficiency and performance. Because of the advanced techniques related to cybercrimes, innumerable amounts of privacy and security issues appeared. From this time, a novel concern has been identified and recognized, i.e., the concept of

cyber security. Cyber security is a significant concept due to the rise and evolution in information technology (Leszczyna, Wallis, & Wróbel, 2019). For that reason, data privacy and security have been viewed as the most substantial sanctuary for all kinds of organizations. The business of all people is done within the boundaries of a worldwide site where important and unimportant information and data are located in a digital format or in a commonplace where all data and information are stored, i.e., international clouds. Social systems provide a chance through which the users will be contented among support systems and domestic participants. When individuals use social networks, they needn't take all measurements the same as the banking or security sector fields (Mittal, 2020). Important structures of management, governments, services, cash related fundamentals, emergency treatment centers and diverse businesses are employing safekeeping procedures, strategies to sustain the going up degree and embarrassing situation of alphanumeric attacks and safeguard secluded information pack up in archives, structures and online devices (Culot, Fattori, Podrecca, & Sartor, 2019). Businesses can protect their private information and data by employing cyber security systems, e.g., security PIN, verification ways and anti-viruses (Nam, 2019). Considering the importance and impactful outcome of awareness and training, following two hypotheses have been generated.
H4: Awareness mediates Cyber security effectiveness to organisational efficiency
H5: Employee Training on Cyber Security enhance organisational efficiency

Methodology

This research aims to assist the organizations top management to coordinate and organize individuals, technology, operations and processes to reach information security goals within an organization. Since this research is analytical and empirical, a descriptive method is applied to designate and describe the population's characteristics. To measure the variables, a structured questionnaire based on the hypotheses as well as previous studies related to the subject of this research and prepared by the researcher by using (365 Microsoft forms) and distributed through email accounts and social media accounts. The respondents included the India and MENA countries (Algeria, Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, United Arab Emirates and Yemen) on public employees, private sectors, academicians located in the Indian and MENA countries.

Sampling Techniques

The sampling technique is substantial as financial plan and time plan limitations do not give the opportunity of surveying the entire population. Sampling can provide the researcher with greater straightforwardness as well as speedy results (Trim & Lee, 2019). A structured instrument was administered to collect respondents' feedback on data security practices, perceived security, response efficiency, perceived usefulness, perceived behavioral control, awareness, and cyber security training and efficiency. These scales were measured considering 5-point liker scale (Strongly agreed to strongly disagree). The researchers applied a field study on

employees of public and private sectors from India and MENA countries. This study applied the Multistage sampling technique by dividing the population into various groups. The sample was stratified based on their age, gender, qualification, and sectors, which enabled the researchers to reach the possible participants. A structural equation model is administered to explain the relationship between information systems and organisational effectiveness.

Data Collection

The population for the research were employees working in various public and private sectors. Since data was collected across Indian and MENA countries, samples have been distributed as per the proportion considering data published in the ministry of labor and labor regulation authority. Considering the current pandemic, questionnaires have been distributed through social media and emails. The appropriate tool was selected and examined to fit this research and suit this study's hypotheses for collecting primary data. The researchers developed a questionnaire in order to accomplish the study objectives. The study population consists of public employees, public employees, private sectors, academicians located in India and MENA countries. Accordingly, this study employed a convenience sampling technique. The study sample consists of 200 employees from public and private sectors.

Table 1. Factors of Cronbach's Alpha and KMO.

Sl. No	Factors	No. of Items	Cronbach's Alpha	KMO
1.	Employee Training on Cyber Security	3	0.767	0.694
2.	Cyber Security Challenges Related to Threats	5	0.817	0.705
3.	Cyber Security Challenges Related to Experience	12	0.936	0.886
4.	Data Security Practices	4	0.896	0.778
5.	Vulnerability	3	0.806	0.666
6.	Perceived Severity	3	0.868	0.697
7.	Response Efficacy	3	0.840	0.694
8.	Data Self-Efficacy	4	0.882	0.776
9.	Awareness	4	0.880	0.786
10.	Perceived usefulness	3	0.849	0.708
11.	Perceived Ease of Use	3	0.836	0.713
12.	Subjective Norms	3	0.767	0.694
13.	Perceived Behavioral Control	3	0.817	0.705
14.	Efficiency	8	0.936	0.886
15.	Employees' Level of Agreement	18	0.907	0.916

Cronbach's Alpha test was applied on all questionnaire items, and the least acceptable level is Alpha $\geq$ 0.60, according to Sekaran & Bougie (2016). The researchers also used A Kaiser-Meyer-Olkin (KMO) test used in research to

determine the sampling adequacy of data to be used for Factor Analysis. Social scientists often use Factor Analysis to ensure that the variables they have used to measure a particular concept are measuring the concept intended. KMO values are between 0.60 and 1, indicating that the sampling is adequate (Reading & Aspects, 2008).

Results

The study was discussed the demographic profile, cyber security awareness and practices. This discussion was presented through Tables and explained as follows.

Table 2. Results of Hypotheses and analysis of model

Hypotheses path	SE	CR	P Value	Result
Data security practices enhances organisational efficiency	0.072	-4.265	0.001	Supported
Perceived Severity and Subjective Norms enhance efficiency	0.062	-4.253	0.001	Supported
Perceived Behavioral Control and Response Efficacy increase efficiency	0.162	-5.125	0.000	Supported
Awareness mediates Cyber security effectiveness to organisational efficiency	0.192	-6.120	0.002	Supported
Employee Training on Cyber Security enhance organisational efficiency	0.099	-4.235	0.001	Supported

P=0.005; TLI=0.952; CFI=0.821; RMSEA=0.05; X^2=402.071; df=423

The results of the hypotheses in Table 2 state that all hypotheses support the overall impacts on organisational efficiency. The outcome of this study indicates that variables like data security practices, which are part of organisational policy and procedure, contribute to efficiency in all operational activities. Similarly, in Hypothesis 2, Perceived Severity and Subjective Norms enhance efficiency. On the other hand, perceived behavioral control and response efficacy also contribute to increasing organisations' efficiency. One of the key factors in generating effective

performance is organisationsl awareness program and training and development activities that enhance efficiency.

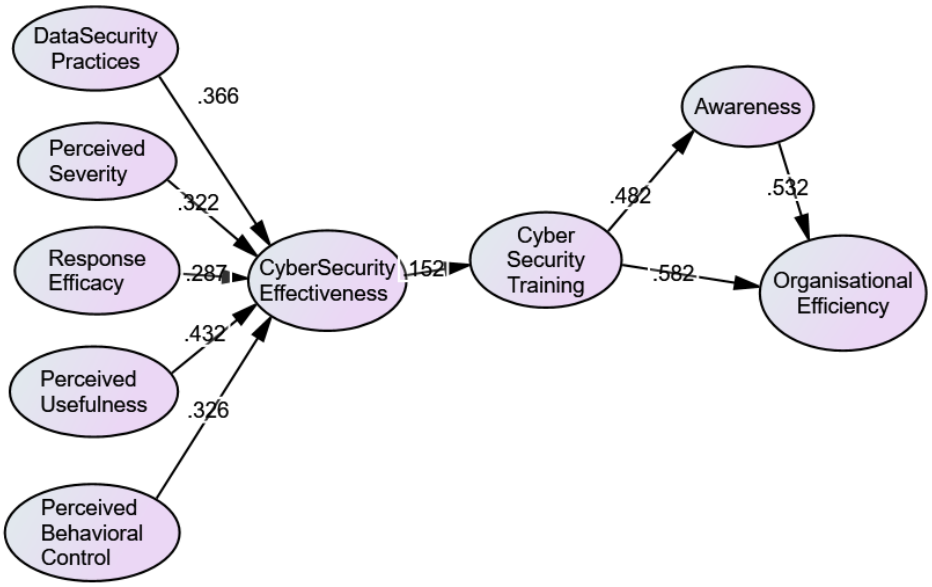

Figure 1: Structural Equation model

This study performed a structural equation model using AMOS to validate the research measures (Figure 1). The Confirmatory factor analysis was disseminated, and with all the measurement techniques like root mean square error of approximation, Akaike's information criterion, Tucker-lewis index used to measure the adequacy. CFI, TLI and RMSEA values were found to be above .90 and .08, which are benchmarks to represent goof fit (Hair Jr., Matthews, Matthews, & Sarstedt, 2017; Kolenikov, 2009).

Table 3. Demographic Profile

Variables	Frequency	Percent
20-25	38	19.0
26-35	101	50.5
36 to Above	61	30.5
Male	101	50.5
Female	97	48.5
I'd rather not say	2	1.0
High school graduate	4	2.0

Some college	6	3.0
Associates degree	9	4.5
Bachelor	154	77.0
Masters or Professional degree	23	11.5
Doctorate	4	2.0
Total	200	1.0

As per Table 3, employees working for the public sector is 101 employees that represent 50.5% of all respondents aged from 26 to 35 years old, whereas the lowest percentage is 19%, representing employees' ages between 20 and 25 years old. Moreover, the percentage of male employees is approximately equal to the percentage of female employees with a slight prominence of the male gender. The male employees are 50.5%, while the female employees are 48.5%. That is with 1% preservative participants who prefer not to say their gender as a matter of privacy. In addition, bachelor's degree is 77%, while the lowest number of employees have a high school degree with a percentage of 2%. It is also seen that employees who hold a PhD are only 2 percentage.

Table 4. Level of Cyber Security Awareness

Factors	Mean	P value
Data Security Practices	3.67	0..002**
Vulnerability	3.69	0.008**
Perceived Severity	3.76	0.000*
Response Efficacy	3.70	0.023**
Data Self-Efficacy	3.70	0.031**
Awareness	3.74	0.000*
Perceived Usefulness	3.74	0..002**
Perceived Ease of Use	3.72	0.001**
Subjective Norms	3.61	0.001**
Perceived Behavioral Control	3.71	0.022**
Efficiency	3.70	0.021**
Note: **denotes significant at 1% level, *denotes significant at 5% level.		

Table 4 explains the factors mean values and their p values, and all the factors are significant at 0.1 level and 0.5 level. Table 4 also describes each variable mean of each factor. The data describe the context of data security practices. The overall average of the respondents is 3.670 with verbal interpretation agree, which indicates that the majority of the respondents agree that data security practices affect the level of cyber security awareness. In the context of vulnerability, the overall average of the respondents is 3.695 with a verbal interpretation of Agree, which indicates that most respondents agree that there is a positive relationship between vulnerability and the level of cyber security awareness. The perceived severity of the overall average of the respondents is 3.763 with verbal interpretation agree which indicates that the

majority of respondents agree that there is a positive relationship between perceived severity and the level of cyber security awareness. The factor of response efficacy, the overall average of the respondents, is 3.701 with verbal interpretation agree, which indicates a positive relationship between response efficacy and the level of cyber security awareness.

The data self-efficacy, the overall average of the respondents, is 3.705 with verbal interpretation agree which indicates that there is a positive relationship between data self-efficacy and the level of cyber security awareness. In the context of awareness, the overall average of the respondents is 3.708 with verbal interpretation agree. In the matter of perceived usefulness, the overall average of the respondents is 3.743 with verbal interpretation agree. It is. Also, the highest average is for employees who choose that exercising care before opening email attachments effectively prevents viruses from infecting the data, with an average of 3.77. In concern of perceived ease of use, the overall average of the respondents is 3.740 with verbal interpretation agree. In the context of subjective norms, the overall average of the respondents is 3.728 with verbal interpretation agree. Moreover, in the context of perceived behavioral control, the overall average of the respondents is 3.616 with verbal interpretation agree. It can also be seen that the highest average is for employees who choose that their family and friends believe that it is difficult to check emails or files for viruses or suspicious material for them with an average 3.64. In addition to that, efficiency, the overall average of the respondents, is 3.71 with verbal interpretation agree.

Discussion

According to the study results, it has been found that a larger part of the respondents is the employees of public sector in accordance with the components of cyber security awareness level (data security practices, vulnerability, perceived severity, response efficacy, data self-efficacy, awareness, perceived usefulness, perceived ease of use, subjective norms, and efficiency). It has been found that most of the employees agree that data security practices are important components of cyber security awareness. The most significant finding is related to dealing with an email attachment with much caution as it may contain a virus. These results are much consistent with the results of previous literature (Chigada & Daniels, 2021), which stated that a considerable amount of trespasses related to security initiate, principally, from within the firm as a result of the manipulators' unawareness or uncaring practices, e.g. unrestrained passcodes, weak passwords and opening an unidentified email. These practices become habits and work styles. Unfortunately, such uncaring practices may expose the firm to considered hackers' threats as well as endanger the firm's resources. Also, it has been found that the majority of the employees agree that vulnerability is an important component of cyber security awareness. Public employees state that the chances of receiving an email attachment with a virus are high. These results are consistent with an earlier study that stated that phishing has

been exposed to more advanced threats (Nair, Alshaikh, & Culnane, 2020). The attackers utilize hoaxed emails and mock-up websites to access private information. The research recognised most of the respondent's perceived severity is an important component of cyber security awareness. Public employees state that the data is infected by a virus as a result of opening a suspicious email attachment, daily work could be negatively affected. In the same context, it has been found that the majority of the employees agree that response efficacy is an important component of cyber security awareness. Public employees state that in case of receiving a suspicious email, I can react effectively in a timely manner. These results are much consistent with the study of Kour and Karim (2020), which states that even though programmed arrangements may be exploited to recognize seriously fake emails as well as websites, those schemes cannot utterly and precisely become aware of phishing attackers. It has been found that the majority of the employees agree that data self-efficacy, perceived usefulness, perceived ease of use and subjective norms and efficiency are major components of cyber security awareness level. The majority of employees agree that investing in learning and developing skills for data security is an essential quality everyone should have. They also agree that supervisors at work believe that data security is very important. To a great extent, these results are consistent with (Chittister & Haimes, 2020), who state that unceasing information security attentiveness and awareness is necessary to endure a necessary level of information and data security attentiveness.

It has been found that the majority of the employees agree that the purpose of training within the respondents is to raise desired behavioral changes and motivation as well as enhance traditional training programs. These results are, to a great extent, consistent with (Trim & Lee, 2019), who see that training programs are viewed as the most critical portion of the managerial set-ups of a safe information processing atmosphere as they help employees to satisfy their motivational, cultural and behavioral desire. In the same way, Caldwell et al. (2019) conducted an investigation that showed the importance of training programs and found that these programs reinforce the motivation level of employees (Caldwell et al., 2019). It has been found that, as per the respondents, the majority of the employees agree that the most important limitation facing the cyber security training employees' programs are both time and budget. These results are, to a great extent, consistent with (Chigada & Daniels, 2021), who states that financial issues play a very critical role when an organization wants to train its staff. It has been found that, as per the respondents, the majority of the employees agree that the most important benefits gained from cyber security training programs are the enhancing of care when reading emails with attachments. They also agree that training programs are not considered time-consuming. These results are, to a great extent, consistent with (Sarı, Güleş, & Yiğitol, 2020), who find that training programs related to cyber security tend to increase the watchfulness of employees against phishing. It has been found that, as per the respondents, the majority of the employees agree that the most critical scales exposed to threats from cyber security attacks are the networks and the electronic

systems. To a great extent, these results are on par with (Chittister & Haimes, 2020), who observe that there have been so many scales exposed to cyber-attacks and cyber-threats and arising from well-thought-out criminalities, which are the networking systems.

Conclusion

The internal consistency of the Study Questionnaire by presenting the Kaiser Mayer Olkin and Cronbach Alpha Test of the questionnaire has proved that the questionnaire used is reliable and internally consistent. Then, the researchers discussed the descriptive analysis of the study. The first part of the descriptive analysis included demographic characteristics (ages, genders, major under the correct college, highest level of education, IT knowledge/experience, level within the organization and employees' organization size). After that, the researchers have discussed the other variables, level of cyber security awareness and analysis of the data collected from the respondents, which focus on threats and challenges, and analysis of the data collected from the public and private sectors. This study has found the impact of effective cyber security and information system on organisational efficiency. The hypotheses and results proved that key variables like data security practices, vulnerability, perceived severity, response efficacy, data self-efficiency, perceived usefulness, and subjective norms significantly impact the effectiveness of cyber security in organisations. This study statistically evaluated the mediating factor using the structural equation model and found that effective training on cyber security and creating awareness in the organisation regarding cyber security risk generate efficiency in all operational tasks.

Industry 4.0 is paving the way for a legacy that is loaded with technology. The advent of technology invariably calls for newer methods to protect the interests of the stakeholders and hence keep a high thrust on cyber security. This research article has tapped on certain basic details of the cyber security needs but was confined to a smaller sample. The researchers can conduct the same study at a global level and make a comparative analysis based on the area of operations and the need for growth. A larger perspective can help in increasing the use of IoT, AI and cyber-physical systems and thus contribute no increasing the industry efficiency.

Reference

Aghakhani, N., Roshani, R., Zarei, A., Delirrad, M., Rahbar, N. and Cheraghi, R., (2020). Analysis of occupational injuries in employees of forensic medicine organizations of West Azerbaijan province in 2016. *Iran Occupational Health*, *16*(6), 16–26.

Al-Gasawneh, J.A., Anuar, M.M., Dacko-Pikiewicz, Z., Saputra, J. (2021). The impact of customer relationship management dimensions on service quality. *Polish Journal of Management Studies*, 23 (2), 24-41.

Anand, R., Medhavi, S., Soni, V., Malhotra, C. and Banwet, D. K., (2018). Transforming

information security governance in India (A SAP-LAP based case study of security, IT policy and e-governance). *Information and Computer Security*, *26*(1), 58–90.

Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M. F., (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*. Bin, J., Joint, J., Academy, E. D., & Emirates, U. A. (n.d.). *New Security Dynamics in the Gulf and the Transformation of the GCC States ' Security Agenda*. 1–10.

Bhatt, D., Danalakshmi, D., Hariharasudan, A., Lis, M. and Grabowska, M., (2021). Forecasting of energy demands for smart home applications. *Energies, 14*(4): 1045.

Caldwell, B. S., Nyre-Yu, M. and Hill, J. R., (2019). Advances in human-automation collaboration, coordination and dynamic function allocation. *Advances in Transdisciplinary Engineering*, *10*, 348–359.

Cao, C.-P., Huang, H., Yu, Y.-H. and Huo, F., (2014). Practice and thinking of quality management of organ procurement organization. *Chinese Journal of Tissue Engineering Research*, *18*(36), 5891–5895.

Chigada, J., Daniels, N., (2021). Exploring information systems security implications posed by BYOD for a financial services firm. *Business Information Review*.

Chittister, C. G., Haimes, Y. Y., (2020). The Role of Modeling in the Resilience of Cyberinfrastructure Systems and Preparedness for Cyber Intrusions. *Journal of Homeland Security and Emergency Management*, *8*(1).

Culot, G., Fattori, F., Podrecca, M. and Sartor, M., (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*, *47*(3), 79–86.

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P. and Utakrit, N., (2021). A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. *2021 2nd International Conference on Smart Computing and Electronic Enterprise: Ubiquitous, Adaptive, and Sustainable Computing Solutions for New Normal, ICSCEE 2021*, 102–106.

Gontar, P., Homans, H., Rostalski, M., Behrend, J., Dehais, F. and Bengler, K., (2018). Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior. *Journal of Air Transport Management*, *69*, 26–37.

Hair Jr., J. F., Matthews, L. M., Matthews, R. L. and Sarstedt, M., (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107.

Ingalagi, S. S., Nawaz, N., Rahiman, H. U., Hariharasudan, A. and Hundekar, V., (2021). Unveiling the crucial factors of women entrepreneurship in the 21st century. Social Sciences, 10(5), 153.

Jibril, A.B., Kwarteng, M.A., Appiah-Nimo, C., Pilik, M. (2019). Association rule mining approach: Evaluating pre-purchase risk intentions in the online second-hand goods market. *Oeconomia Copernicana*, 10(4), 669-688.

Kolenikov, S., (2009). Confirmatory factor analysis using confa. *Stata Journal*, *9*(3), 329–373.

Kour, R., Karim, R., (2020). Cybersecurity workforce in railway: its maturity and awareness. *Journal of Quality in Maintenance Engineering*, *27*(3), 453–464.

Kralj, D., (2010). The role of environmental indicators in environmental management. *International Conference on Circuits, Systems, Signals, CSS*, 139–145.

Lazanyi, K., Lambovska, M., (2020). Readiness for Industry 4.0 Related Changes: a Case Study of the Visegrad Four. *Ekonomicko-Manazerske Spektrum*, *14*(2), 100–113.

Leszczyna, R., Wallis, T. and Wróbel, M. R., (2019). Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre. *Decision Support Systems*, *122*.

Litchfield, I. J., Bentham, L. M., Lilford, R. J., McManus, R. J., Hill, A. and Greenfield, S., (2017). Adaption, implementation and evaluation of collaborative service improvements in the testing and result communication process in primary care from patient and staff perspectives: A qualitative study. *BMC Health Services Research*, *17*(1).

M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y. and Miyamoto, D., (2019). A normative decision-making model for cyber security. *Information and Computer Security*, *26*(5), 636–646.

Mahadevan, V., Agbinya, J. and Braun, R., (2006). Analyzing usability alternatives in multi-criteria decision making during ERP training. *7th International Conference on Information Technology Based Higher Education and Training, ITHET*, 296–309.

Mantha, B. R. K., García de Soto, B., (2021). Assessment of the cybersecurity vulnerability of construction networks. *Engineering, Construction and Architectural Management*, *28*(10), 3078–3105.

Mathiesen, P., Marjanovic, O., Delavari, H. and Bandara, W., (2013). A critical analysis of business process management education and alignment with industry demand: An Australian perspective. *Communications of the Association for Information Systems*, *33*(1), 463–484.

Mittal, H., (2020). How Does the Institutional Context of an Emerging Economy Shape the Innovation Trajectory of Different Types of Companies? a Case Study of India. *Ekonomicko-Manazerske Spektrum*, *14*(2), 36–51.

Nam, T., (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*.

Nica, E., Potcovaru, A.-M. and Hurdubei Ionescu, R. E., (2019). Resilient cyber-physical systems and big data architectures in industry 4.0: Smart digital factories, automated production systems, and innovative sustainable business models. *Economics, Management, and Financial Markets*, *14*(2), 46–51.

Porcedda, M. G., (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer Law and Security Review*, *34*(5), 1077–1098.

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil and Dwivedi, Y. K., (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*.

Reading, F., Aspects, M., (2008). Spearman Rank Correlation Coefficient. Concise Encycl. *Stat*, 502–505.

Rowland, Z., Krulicky, T. and Oliinyk, O., (2020). Capital Cost Quantification Model in Business Activity Planning: the Evidence of the Middle Europe Countries. *Ekonomicko-Manazerske Spektrum*, *14*(1), 30–42.

Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J. J. M., (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39.

Sarı, T., Güleş, H. K. and Yiğitol, B., (2020). Awareness and readiness of Industry 4.0: The case of Turkish manufacturing industry. *Advances in Production Engineering And Management*, *15*(1), 57–68.

Sekaran, U., Bougie, R., (2016). *Research methods for business: A skill building approach*.

John Wiley & Sons.
Sujith Kumar, M., Vishal Gupta, N., Balamuralidhara, V., Biswas, S., Pramod Kumar, T. M. and Naga Krishna Teja, I., (2011). Compilation of key GMP requirements in us and Japan for tablet manufacturing. *International Journal of Drug Development and Research*, *3*(4), 45–54.
Trim, P. R. J., Lee, Y.-I., (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224–238.
Zauskova, A., Lyakina, M., Tretyak, V. and Miklencicova, R., (2020). Application of Artificial Neural Networks To Cost Factors Stimulating Innovation – the Case of Slovakia. *Ekonomicko-Manazerske Spektrum*, *14*(1), 97–105.

SKUTECZNY SYSTEM INFORMACYJNY I EFEKTYWNOŚĆ ORGANIZACYJNA

Streszczenie: Niniejsze badanie ma na celu określenie skuteczności systemów informatycznych w zakresie sprawności organizacyjnej w perspektywach technicznych i operacyjnych w różnych sektorach publicznym i prywatnym. Nowość badania koncentruje się na praktykach w zakresie bezpieczeństwa danych, postrzeganej dotkliwości, skuteczności reakcji, postrzeganej użyteczności i postrzeganej kontroli behawioralnej nad efektywnością organizacji. Dane ankietowe zostały zebrane od 200 specjalistów reprezentujących sektor publiczny i prywatny w Indiach i krajach MENA, którzy szeroko popierają te wyniki. Analiza danych została wygenerowana przez zastosowanie modelu równania i różnych opisowych narzędzi statystycznych przy użyciu AMOS i SPSS. Wyniki badania pokazują, że skuteczny system informacyjny z kompleksowym zarządzaniem informacją pozwala uniknąć potencjalnych cyberataków i poprawia wydajność organizacji. Badanie wykazało, że powtarzające się cyberataki zagrażają reputacji firmy i jej działaniom organizacyjnym. Dlatego budowanie wśród pracowników skutecznej świadomości na temat zagrożeń i wyzwań związanych z działalnością biznesową zwiększa wydajność i efektywność organizacji. To badanie empiryczne w znacznym stopniu przyczyniło się do podkreślenia przez organizacje odpowiednich środków w celu włączenia skutecznych informacji i planu łagodzenia ryzyka w celu ochrony danych i wydajności. Wyniki badań podkreślają, że szkolenie i świadomość są zmiennymi pośredniczącymi w zwiększaniu wydajności.

Słowa kluczowe: cyberbezpieczeństwo, internet myślenia, cyberryzyko, socjotechnika, Indie, MENA

有效的信息系统和组织效率

摘要：本研究旨在确定信息系统在各个公共和私营部门的技术和运营角度对组织效率的有效性。该研究的新颖之处在于数据安全实践、感知严重性、响应效率、感知有用性和感知对组织有效性的行为控制。调查数据来自代表印度和 MENA 国家公共和私营部门的 200 名专业人士，他们广泛支持这些结果。数据分析是通过应用方程模型和使用 AMOS 和 SPSS 的各种描述性统计工具生成的。研究结果表明，具有全面信息管理的有效信息系统可以避免潜在的网络攻击并提高组织的绩效。该研究发现，反复的网络攻击会威胁到企业及其组织运营的声誉。因此，在员工中建立对业务运营风险和挑战的有效意识可以提高组织的绩效和效率。这项实证研究为组织强调采取适当措施以纳入有效信息和风险缓解计划以保护数据和效率做出了重大贡献。研究结果强调，培训和意识是提高绩效的中介变量。

关键词: 网络安全, 思维互联网, 网络风险, 社会工程学, 印度, MENA