


**FORMULATING THE CYBER SECURITY CULTURE IN ORGANIZATIONS: PROPOSING AND ARGUING INSIGHTS**

**Saeed Hameed Aldulaimi<sup>A</sup>, Marwan Mohamed Abdeldayem<sup>B</sup>, Mohammed Yousif Abo Keir<sup>C</sup>**



ARTICLE INFO	ABSTRACT
<p><b>Article history:</b></p> <p><b>Received</b> 20 February 2023</p> <p><b>Accepted</b> 08 May 2023</p>	<p><b>Purpose:</b> This research aims to enhance practical organizational practices and academic research literature by critically investigating the latest findings in cybersecurity culture research through a systematic review of relevant literature and research.</p>
<p><b>Keywords:</b></p> <p>Cybersecurity Culture; Information Security Culture; Organisational Culture; Management.</p>	<p><b>Theoretical Framework:</b> This work seeks to summarize key research developments in a research area that remains challenging for companies as they seek to build strong security cultures to protect their information (Tripwire, 2020). And reviewing the legal regulations that must be trained to protect institutions from cyber threats in the Kingdom of Bahrain and Saudi Arabia.</p>
	<p><b>Design/Methodology/Approach:</b> The methodology of this study implements a systematic literature review to assess the main components of cybersecurity culture and what good practice can help to build it professionally.</p> <p><b>Findings:</b> The main results find that current literature must move from a technical approach to information security to a socio-cultural one. Also, this study predicts that cybercrime will increase dramatically and cost the world trillions annually.</p> <p><b>Research Practical and Social Implications:</b> this study attempts to define human resource management's role in cybersecurity awareness training and therefore the managers can develop the necessary rules to secure the organizational information.</p> <p><b>Originality/Value:</b> The study is within the first studies to be conducted in GCC countries. Moreover, the to build a cyber security culture is unique topic add on to the academic knowledge. Also, can motivate the future studies to focus on efficiently organizing security procedures and enhancing security readiness appraisal consequences by providing more perceptions of imminent threats and security hazards.</p> <p>Doi: <a href="https://doi.org/10.26668/businessreview/2023.v8i5.1660">https://doi.org/10.26668/businessreview/2023.v8i5.1660</a></p>

**FORMULANDO A CULTURA DE SEGURANÇA CIBERNÉTICA NAS ORGANIZAÇÕES: PROPOR E DISCUTIR INSIGHTS**

**RESUMO**

**Objetivo:** Esta pesquisa visa aprimorar as práticas organizacionais práticas e a literatura de pesquisa acadêmica, investigando criticamente as descobertas mais recentes na pesquisa da cultura de segurança cibernética por meio de uma revisão sistemática da literatura e pesquisa relevantes.

**Referencial Teórico:** Este trabalho busca resumir os principais desenvolvimentos de pesquisa em uma área de pesquisa que continua desafiadora para as empresas, pois buscam construir fortes culturas de segurança para

<sup>A</sup> Associate Professor. Applied Science University (ASU). Kingdom of Bahrain.

E-mail: [saeed.aldulaimi@asu.edu.bh](mailto:saeed.aldulaimi@asu.edu.bh) Orcid: <https://orcid.org/0000-0003-1131-5633>

<sup>B</sup> Associate Professor. Applied Science University (ASU). Kingdom of Bahrain

E-mail: [Marwan.abdeldayem@asu.edu.bh](mailto:Marwan.abdeldayem@asu.edu.bh) Orcid: <https://orcid.org/0000-0002-9103-9802>

<sup>C</sup> Associate Professor. Applied Science University (ASU). Kingdom of Bahrain

E-mail: [Mohammed.yousif@asu.edu.bh](mailto:Mohammed.yousif@asu.edu.bh) Orcid: <https://orcid.org/0000-0002-9546-4945>

proteger suas informações (Tripwire, 2020). E revisando os regulamentos legais que devem ser treinados para proteger as instituições de ameaças cibernéticas no Reino do Bahrein e na Arábia Saudita.

**Design/Methodologia/Abordagem:** A metodologia deste estudo implementa uma revisão sistemática da literatura para avaliar os principais componentes da cultura de cibersegurança e quais boas práticas podem ajudar a construí-la profissionalmente.

**Resultados:** Os principais resultados indicam que a literatura atual deve passar de uma abordagem técnica da segurança da informação para uma sociocultural. Além disso, este estudo prevê que o cibercrime aumentará dramaticamente e custará trilhões ao mundo anualmente.

**Implicações práticas e sociais da pesquisa:** este estudo tenta definir o papel da gestão de recursos humanos no treinamento de conscientização sobre segurança cibernética e, portanto, os gerentes podem desenvolver as regras necessárias para proteger as informações organizacionais.

**Originalidade/Valor:** O estudo está entre os primeiros estudos a serem conduzidos nos países do CCG. Além disso, a construção de uma cultura de segurança cibernética é um tópico único adicionado ao conhecimento acadêmico. Além disso, pode motivar os estudos futuros a se concentrarem na organização eficiente dos procedimentos de segurança e no aprimoramento das consequências da avaliação da prontidão da segurança, fornecendo mais percepções de ameaças iminentes e riscos à segurança.

**Palavras-chave:** Cultura de Cibersegurança, Cultura de Segurança da Informação, Cultura Organizacional, Gestão.

## FORMULACIÓN DE LA CULTURA DE CIBERSEGURIDAD EN LAS ORGANIZACIONES: PROPUESTA Y DISCUSIÓN DE INSIGHTS

### RESUMEN

**Propósito:** esta investigación tiene como objetivo mejorar las prácticas organizacionales prácticas y la literatura de investigación académica mediante la investigación crítica de los últimos hallazgos en la investigación de la cultura de la seguridad cibernética a través de una revisión sistemática de la literatura y la investigación relevantes.

**Marco teórico:** este trabajo busca resumir los principales desarrollos de investigación en un área de investigación que sigue siendo un desafío para las empresas, ya que buscan construir culturas de seguridad sólidas para proteger su información (Tripwire, 2020). Y repasando las normativas legales que deben estar capacitadas para proteger a las instituciones de las amenazas cibernéticas en el Reino de Bahrein y Arabia Saudita.

**Diseño/Methodología/Enfoque:** La metodología de este estudio implementa una revisión sistemática de la literatura para evaluar los principales componentes de la cultura de ciberseguridad y qué buenas prácticas pueden ayudar a construirla profesionalmente.

**Resultados:** Los principales resultados indican que la literatura actual debe pasar de un enfoque técnico de la seguridad de la información a uno sociocultural. Además, este estudio predice que el delito cibernético aumentará drásticamente y le costará al mundo billones de dólares anualmente.

**Implicaciones prácticas y sociales de la investigación:** Este estudio trata de definir el papel de la gestión de recursos humanos en la formación de la conciencia de ciberseguridad y, por lo tanto, los gerentes pueden desarrollar las reglas necesarias para proteger la información organizacional.

**Originalidad/Valor:** El estudio se encuentra entre los primeros estudios realizados en los países del CCG. Además, la construcción de una cultura de ciberseguridad es un tema único agregado al conocimiento académico. Además, puede motivar a estudios futuros a centrarse en organizar de manera eficiente los procedimientos de seguridad y mejorar las consecuencias de la evaluación de la preparación para la seguridad, brindando más información sobre las amenazas inminentes y los riesgos de seguridad.

**Palabras clave:** Cultura de Ciberseguridad, Cultura de Seguridad de la Información, Cultura Organizacional, Gestión.

### INTRODUCTION

The revolution of the Industrial Internet of Things (IIoT) leads to reshaping the business landscape due to the existence of massive data and security issues (Boyes et al., 2018). The matter of cybersecurity is one of the new vital topics that have arisen in light of the tremendous

development in the technological revolution and our entry into the digital world. Cybersecurity is the current successful approach to maintaining the confidentiality of the organization's information, and from it high levels of protection are built for each of the computers, networks, or programs. Solms and Van Niekerk (2013) define cybersecurity as the goal to protect an additional set of assets, in particular human and organizational assets, which can be considered more comprehensive. The shared values, beliefs and expected behaviors regarding protection can therefore be viewed in this broad range of aspects (Ioannou et al. 2019).

The concept of (security) constitutes an essential concern for specialists in the study of the concept and decision-makers alike. The definition of security linguistically is that it is stated in the language dictionaries that security is the opposite of fear, and from it, safety and trust, and it was said that you are safe from that, i.e. safe. And security means any actions through which society seeks to preserve its right to survive, and it is also the ability by which the institution can secure all its sources and resources. Security is the first need in human perception, which he seeks to achieve after satisfying his basic biological needs. Two opposites are affected by several subjective and objective factors (Al-kaeud, Israa shareef 2022; Azevedo, A. 2018). In order to ensure the achievement of high levels of anticipation and adequacy, the organization has followed the adoption of a comprehensive view of cybersecurity by defining the roles and responsibilities of departments and individuals related to cybersecurity at the level of the entire organization (Hassan et al., 2022). To develop within it and follow up on compliance with national standards in all aspects of cybersecurity with The existence of unified mechanisms for planning, budgeting, and prioritizing effectively in the field of cybersecurity, as well as identifying the affected elements in cyberspace and the severity of the damage, choosing the best ways to treat it or limiting its economic impacts, and defining protection and defense measures according to the degree of danger. The institution also worked on the existence of comprehensive controls and standards to follow up on compliance, which achieves a kind of protection within the cyber security system and continues to enhance that protection through awareness campaigns, as well as strengthening technical capabilities against cyber threats and detecting attacks and threats and recovering from them. According to Hassan et al., 2022; netFlow contains IP flow, Command Line Interface, and NetFlow Collector.

The study conducted by Kaspersky (Kaspersky Lab, 2018), confirmed that 52% of companies report that employees constitute the most significant weakness in terms of cybersecurity. Along with this statement, Verizon's annual report on data breaches (Verizon, 2021) claims that 85% of such violations involve a human component. Therefore, companies

should conduct regular training for all staff to increase cybersecurity mindfulness to prevent or reduce cyber-attacks' impact on business performance and hence the violation of intellectual capital and organizational knowledge (He et al., 2020; Al-Sanjary, O. I., Khalifa, M. 2021).

This research aims to enhance practical organizational practices and academic research literature by critically investigating the latest findings in cybersecurity culture research through a systematic review of relevant literature and research. This work seeks to summarize key research developments in a research area that remains challenging for companies as they seek to build strong security cultures to protect their information (Tripwire, 2020; Thomas, D. C. 2008; Englander, M. 2019). As well as formulating and building an organizational culture that represents a firewall to protect the organization's information sources (Aldulaimi, S. H., & Abdeldayem, M. 2019). In addition to writing the benefits that can be obtained from fortifying the organization with a culture based on creating organizational awareness of the value of information and the danger of the threat from rogues from outside. And it reviewed the legal regulations that must be trained to protect institutions from cyber threats in the Kingdom of Bahrain and Saudi Arabia. Finally, this paper attempts to define human resource management's role in cybersecurity awareness training.

## **LITERATURE REVIEW**

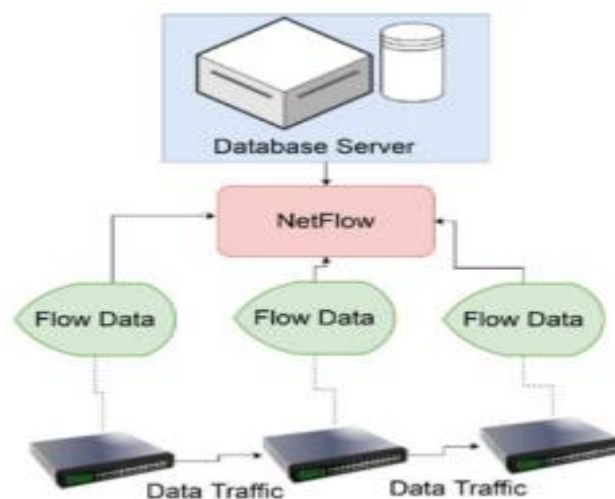
Currently, organizations work hard to promote cybersecurity culture to face an urgent issue in today's business environment, where the practice of smart working is gaining in popularity. Previously, IBM conducted a study (IBM, 2020), and found that the increase in remote working during the COVID-19 pandemic was expected to the escalation of data breach costs and incident response times (Corallo et al., 2022).

There are many benefits that organizations can achieve. Enhancing the protection of information systems and operational technologies at all levels and their components, including hardware and software, as well as the services they provide and the data they contain. Addressing information security attacks and incidents targeting the devices of these institutions. Provide a safe and reliable work environment for transactions in the information society, and the resilience of the infrastructure sensitive to electronic attacks. Eliminate vulnerabilities in computer systems within organizations and mobile devices of all kinds, fill gaps in information systems, and resist malicious software and what it targets to cause great damage to users. Reducing electronic espionage and sabotage at the level of institutions and the individuals working in them, and taking all necessary measures to protect employees and customers alike

from potential risks in the field of various uses of the Internet. Training individuals on new mechanisms and procedures to face the challenges of penetrating the devices of these individuals in order to harm their personal information, whether by destruction or theft (Von Solms, R., & Van Niekerk 2013).

The cultural identity distinguished or recognized those who have similar traditions, language, and basic belief systems (Tongdhamachart & Alwi, 2023). Thus the organizations must embed this kind of norms and beliefs in their culture formula. In Fig. 2, flow-enabled network devices are shown clearly as users enter their inputs and the data is transferred to the server and then to the whole system.

Figure 1: inputs as flow-work network devices



Prepared by the authors (2023).

By training and qualifying employees on cybersecurity techniques and methods, all institutions can benefit in various ways, including protecting the internal internet networks and the institution's data from any unauthorized entry and preventing that it improves its levels of information protection and thus ensures the continuity of its business without any accidents (Darwish, S. 2014). High protection enhances the confidence of both SHAREHOLDERS and stakeholders of the institution. The organization can recover any leaked data as soon as possible in the event of any security breach of the cyber system. Gaining more confidence from the organization's owners in the organization's information security arrangements and methods. Preserving the data and information of the institution with security controls in place globally so that it is not sold or used to steal money. Protecting the business of the institution, where the workers will be able to surf the Internet and receive e-mail without fear of being hacked or threatened, so the work will be completely safe without risks.

## **METHODOLOGY**

In the current study, we implement a systematic literature review to assess the main components of cybersecurity culture and what good practices can help to build it professionally. Analysis of the main techniques used to support companies in achieving compliance with cybersecurity policies and enforcing security-related behavior by employees. Also, identification of the business benefits arising from improved cybersecurity culture within enterprises.

## **CYBER SECURITY PROCEDURE IN SAUDI ARABIA AND BAHRAIN**

The modern world interested to develop the digital era and GCC countries in particular desire to move forward in the digitalization index overwrd and improve the E-Service Quality to promote Institutional Excellence ( Alsuwaidi & Sultan 2023). Comparing what is applied in the Kingdom of Saudi Arabia and the Kingdom of Bahrain, we find that the common regulations, which are considered essential in the field of "cyber security", all aim to provide the necessary needs and requirements so that each organization can protect its networks, associations and applications in order to address all threats. These regulations can be summarized in several points. as follows:

1. Determine the objectives, responsibilities and role of everything related to cyber security in the organization, and ensure the application of its requirements by clarifying security policies
2. Develop training plans, educational programs, or videos in cybersecurity for all employees and even senior management of the institution, and prepare special training programs for that based on the nature of the work assigned to the employees.
3. Providing means of protection for internal systems, networks, and applications, managing security gaps, countering hacking, encryption, and protecting social media accounts.
4. Monitoring the security records of the systems to detect hacking attempts, and defining procedures for dealing with security incidents in order to contain them and reduce the negative impacts on the organization.
5. Developing the necessary requirements to protect the information in the event that it is allowed for the employees of the institutions. The section also presents the protection controls related to cloud computing services, if used.

6. Determine the procedures for the internal and external audit process at the enterprise level to ensure compliance with the application of cybersecurity controls and policies.
7. Preserving the confidentiality of data and information and setting penalties in the event of violating this. The employee must be committed to protecting all the data of the institution, whether financial or not, or related to current and future customers because all this data is of great value to the company.
8. Protect the organization's devices and accounts and not leave them unattended
9. .Ensure that the protection devices installed in the organization's devices are updated monthly or as soon as the update icon appears
10. Safe use of e-mail and not opening attachments when you are not sure of the eligibility of the sent mail
11. Communicate with the Sirian Security Department in the event of any suspicious e-mail messages.

## **HRM AND CYBERSECURITY**

The role of human resources management in awareness training in cybersecurity is that cybersecurity is an integral part of the daily tasks of all security leaders. Academic leaders need to understand, discover, and avoid cyber threats that they may face during their daily activities, as well as helping to reach this point .Human resources: as leaders, who must understand the principles and practices of cybersecurity (Abdeldayem et al., 2021). Operations: Institutions and organizations must have a framework for how they deal with electronic attacks .It guides all users, explaining how to identify attacks, protect systems, detect and respond to threats, and recover from successful attacks? Technology: Technology is necessary to give employees and users electronic security tools and programs to protect themselves from electronic attacks. The role of human resource management lies through encouraging the use of cybersecurity tools at the level of the entire company, by motivating them to use these tools for the purpose of protection or security via the Internet, and working to convince them of the ease of applying these tools and other desired benefits .Informing citizens of the do's and don'ts of cybersecurity, by providing ideas, do's and don'ts, updating devices on a regular basis, removing weaker links in systems and making full use of available official resources .Implement endpoint security at the enterprise level, by protecting organizational data, customer personal information, and official communications from prying eyes and unwanted electronic fools .Providing training on

cybersecurity to employees, through steps taken by the Human Resources Department to enhance cyberspace through awareness of the latest trends and cybersecurity issues in methods, conducting trainings on cybersecurity programs through cooperation with the cybersecurity department to provide knowledge of cybersecurity to employees .Also, prevention against phishing attacks, by being careful of the consequences of electronic confiscation, so that they are not a victim of fraudsters or thieves via the Internet, and therefore the human resources department must conduct intensive courses in educating employees about electronic confiscation (Darwish, 2014; Chaho, R. M., Aswad, A. 2021)).

Furthermore, the role of human resources management in awareness training in cybersecurity human resources management has a major role in spreading awareness and culture of cybersecurity, and the program can be designed to raise capabilities and cognitive sciences related to cybersecurity by using ADDIE, where it must initially assess and analyze the knowledge and capabilities of the employee and identify the gap or deficiency in that until the special training is assigned on its basis appropriate for them. This can be done in two ways :The first, a questionnaire will be sent to measure the existing knowledge of the employees and it contains 20 questions regarding protection, confidentiality, hacking and attacks .Second, an announcement will be sent about the latest hacking attacks and the way they were carried out, for example, through a link for free training courses. Then, after two weeks, an email will be sent announcing the method of knowing the annual increases mechanism by clicking. On the link in the e-mail, through cooperation with the Systems and Information Department to measure the extent of employees' care and attention to what was sent because the e-mail sent was not from the e-mail subject to the company's internal advertisements .After that, the employees who did not follow the instructions were counted and targeted, and their number was 20 employees. Therefore, the objective is to learning cyber security and the importance of its presence in every organization and what are the latest hacking attacks and modern security vulnerabilities and how to address them, and to determine the time it takes for training will be based on the method of answers of the 20 employees who were chosen on the questionnaire sent to limit the information they have as well, and then comes the stage of development and preparation of the program and preparing the scientific material for training and reviewing it by us in coordination with Cyber Security Department. After that, it is sent to the senior management to approve the budget, training time and place, and after obtaining the approval of the senior management on the training budget and the purpose of its existence, we will have to verify all logistical matters and administrative arrangements before the start of the



training. Human resources with the trainees to measure the effectiveness of the training, as in the fifth stage of the ADDIE model, the program and its effectiveness are evaluated and can be measured in several ways during the training period (Al Alkawi, T., & Ali, B. 2022). Through the interest of the trainees in the training and their keenness to attend the training on time. The extent of their interaction with the trainer and the cognitive information they received from him through the questions and simulations they measured on their reality. The extent of the knowledge enrichment they received through this training. After the training period, the outputs must be measured and whether the program has achieved its goal, whether by sending a questionnaire on the effectiveness of the program and recommending it to the rest of the organization's employees, or is there a change in the behavior of the trainees, and is there an increase in their concern regarding hacking attacks, or the way information is transmitted between them and their colleagues at work, as well as measuring The duration of the training was suitable for all parties or was it punctuated by some boredom and a long time (Abdeldayem et al., 2021). Based on these analyzes, the training program and its effectiveness will be re-examined, and then it will be modified to suit its main objective, which is to increase awareness of the importance of cybersecurity, and therefore we will be able to apply it to other categories of trainees and create other more detailed programs on cybersecurity for students who have completed the training now .Using all the informational and technical assets of the institution for business purposes only and in accordance with acceptable use policies for assets approved by the institution and reporting cyber security incidents and adhering to the proper use policy.

### **Legal Regulations and Cyber Threats**

Establishing the Internet Investigation Department specialized in confronting all crimes and illegal activities that take place through the Internet and social media platforms. Technological confrontation, which is concerned with the Ministry of Communications, which supervises all means of communication within the country through the "National Telecommunications Regulatory Authority" and its function is to protect the cyberspace of persons, entities and state institutions, as information crime, as it targets persons and entities, also strongly targets state systems and institutions. It was also agreed to issue the "UNCITRAL Model" law, as states were convinced of the need to prevent these crimes. The legal and legislative confrontation to combat information crimes and the imposition of deterrent penalties for their perpetrators, where work has been done in cooperation between the Ministries of (Justice, Communications and Interior) to study all the risks and threats resulting from the

illegal use of the Internet. Issuing regulations regulating the communication and information technology sector. Develop model legislation to combat information crime, which can be applied globally, and be usable, with existing legislative measures at the national and regional levels. Proposing draft laws and keeping pace with the rapid development in the communications and information technology sector.

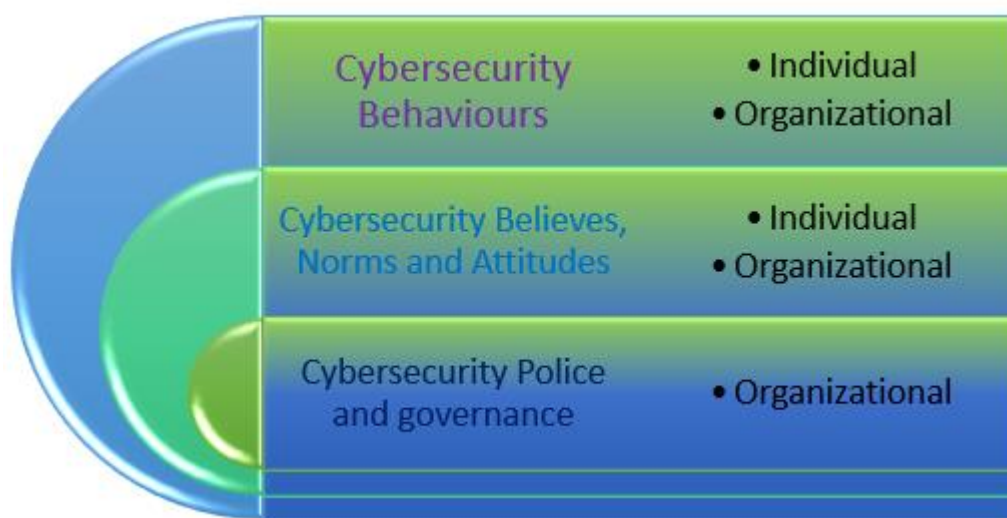
### **Invest in Cyber Security Training**

Investing in the human element is one of the most important methods of advancing development, which is done by ensuring the development of specialized skills and competencies of human resources .In addition to refining the skills of young human cadres in the field of information security, advanced creative designs and data centers, in cooperation with information technology institutes, which will be beneficial to various fields of work by striving to achieve self-sufficiency in competencies trained in all technological methods that are needed in their various lines of business .Moreover, it provides accreditation certificates, training programs in Arabic and English, and special initiatives designed to meet the needs of institutions. And work on the participation of a number of the Center for Secure Electronic Physical Systems in providing training in advanced electronic security, where they will combine their knowledge of electronic security risks, telecommunications infrastructure and information technology limited to the industrial sector, in addition to advanced construction scenarios and capabilities of multiplying high-precision cyber attacks for training (Hassan et al., 2022).

It is known that three factors make training a necessity for any institution, namely development, technical progress, institutional complexity, and human relations, and these three factors are linked to three other factors, as technical progress leads to an increase in the size of the institution and leads to its complexity, and similarly, increasing complexity leads to Increasing technical progress leads at the same time to human problems, and from here training plays the following roles: increasing the effectiveness of workers and employees of the institution, raising morale, achieving better human relations, reducing supervision, increasing the vitality and flexibility of the institution, and introducing new working methods and strategies in the institution, technological advancement ,Institutional policy support (Mohamed, H. M. 2021). Investing in cybersecurity also helps increase productivity and improve the quality of work because it plays the role of the guardian and sponsor of the organization as well as the employees. It is also responsible for building skilled and capable individuals, which helps the

organization to perform its mission and adapt to any new variable, which is what makes institutions spend a lot on training. Also, investing in training employees in cybersecurity would provide a backup force in the organization, reduce accidents, and promote continuity and stability in the organization, and the success of any organization is necessarily linked to training because it is considered an economical means and social prosperity against the inadequacy of individuals for their work. Figure 2 represents the main components of the cybersecurity culture in organizations that the deep content exists in the organization and the manifestations appear clearly in behavior.

Figure 2: Proposed model of cybersecurity culture in organizations



Prepared by the authors (2023).

## CONCLUSION

This work seeks to summarize key research developments in a research area that remains challenging for companies as they seek to build strong security cultures to protect their information—building an organizational culture that represents a firewall to protect the organization's information sources. This research aimed to enhance practical corporate practices and academic research literature by critically investigating the latest findings in cybersecurity culture research through a systematic review of relevant literature and research. In addition, review the legal regulations that must be trained to protect institutions from cyber threats in the Kingdom of Bahrain and Saudi Arabia. Finally, this paper attempts to define human resource management's role in cybersecurity awareness training. The urgent need to improve cybersecurity practices became strong in conjunction with the massive data era. I must maintain that my organization is fully prepared for any security gaps. Still, it strives to keep

pace with technological changes in this field. It has focused on establishing a risk management department that studies all technological risks and directs human resources management in cooperation With the administration of systems and technical information to train and equip all employees for any trouble in the field of cyber security. An organization's most significant threat to privacy and security, even if not acknowledged, is considered to be its staff (Georgiadou et al., 2022; Aldulaimi et al 2021).

This study concludes that current literature must be moved from a technical approach to information security to a socio-cultural system. Also, this study predicts that Cybersecurity cybercrime would increase dramatically and cost the world trillions annually (Georgiadou et al., 2021; Abdeldayem, M. Mohamed and Al Dulaimi, Saeed Hameed. 2022). In all cases, investing in training the employee on every development that takes place in the world is of great benefit to him. It leads to many benefits, including enriching the knowledge of the worker, increasing the level of intellectual awareness, learning new ways to perform tasks, and thus increasing productivity, which is also beneficial to the institution. Among them, we find that setting plans and budgets for training employees Concerning cyber security, is a profitable investment process that benefits the employee first and the institution second.

On the one hand, it makes the employee aware of what is happening in the digital world. It helps him to identify malware and the various forms of cybercrime and hacking attacks. Thus he will be civilized and ready to act safely and responsibly over the Internet and when comparing the performance of those who attended the course before and after it concerning ensuring the protection of the company's technological property And not allowing themselves to be the cause of any security gap in the organization's firewall, and this indicates that their loyalty to the company has increased. Through this, the return on investment can be measured because it is an intangible return, but it can be seen in the performance of employees. Continuous efforts need to be made that evolve on cyber-security culture framework consisting of new models to promote this aspect. Forthcoming studies need to focus on efficiently organizing security procedures and enhancing security readiness appraisal consequences by providing more perceptions of imminent threats and security hazards.

## REFERENCES

Abdeldayem Marwan M, Aldulaimi S. H. (2020) "Trends of Global Fintech Education Practices and the GCC Perspective". *International Journal of Advanced Science and Technology*, Vol. (29), No. (3), Pp. 7150 - 7163.

Abdeldayem, M. M., Al Dulaimi, S. H., & Al Dulaimi, F. H. (2021). A qualitative approach to evaluate the reconciliation of GOLDX and OneGram in Islamic Finance. *Zbornik radova Ekonomskog fakulteta u Rijeci: časopis za ekonomsku teoriju i praksu*, 39(1), 113-134.

Alsuwaidi, S. J., & Sultan, A. A. B. M. (2023). The Impact of E-Service Quality on Institutional Excellence Within abu Dhabi Municipality in UAE. *International Journal of Professional Business Review*, 8(4), e0960. <https://doi.org/10.26668/businessreview/2023.v8i3.960>

Abdeldayem, M. M., Aldulaimi, S. H., & Alazzawi, A. (2021, November). Sustainable Leadership and Academic Excellence: Arab Culture Perspective. In 2021 Sustainable Leadership and Academic Excellence International Conference (SLAE) (pp. 33-37). IEEE.

Abdeldayem, M. Mohamed and Al Dulaimi, Saeed Hameed. (2022) "Predicting crowdfunding economic success in the Gulf Cooperation Council. *International Journal of Engineering Business Management*, Vol. (14), Pp. 1-12

Al Alkawi, T., & Ali, B. J. (2022). Electronic Financial Disclosure Level on the Commercial Bank Sector of Bahrain Bourse. *International journal of green management and business studies*. Vol. 1, No. 2. Pp.52

Aldulaimi, S. H., & Abdeldayem, M. M. (2019) How Changes In Leadership Behaviour And Management Influence Sustainable Higher Education In Bahrain. *International Journal of Scientific and Technology Research*, Vol. (8), No. (11), Pp. 1826-1934.

Aldulaimi, S. H., & Talal, A. A. (2021). Green Technologies of Human Resources for Green Economy: Application on GCC Countries. *International Journal of Green Management and Business Studies*, 1(1), 26-41.

Aldulaimi, S. H., Abdeldayem, M. M., Alazzawi, A., & Abdulrazaq, M. L. (2021, October). Digital Education Industry and Academic Perception to Improve Business Intelligence. *International Conference on Data Analytics for Business and Industry (ICDABI)* (pp. 218-225). IEEE.

Aldulaimi, S. H., & Abdeldayem, M. M. (2018). The economic value of time in Arab culture: New evidence using Zimbardo Time Perspective Inventory (ZTPI). *American Journal of Social Sciences and Humanities*, 3(1), 63-72.

Al-kaeud, Israa shareef (2022) The Cyber Influence of the National Security of the Active Countries (United States of America as a Model), *Political Sciences Journal*, Issue (64) p (1-18).

Al-Sanjary, O. I., Khalifa, M. (2021) Impact of COVID 19 Pandemic on Small and Medium Sized Businesses (SMEs) in the GCC. *International Journal of Green Management and Business Studies*, Vol. (1), No. (1), Pp. 29-49

Ang, S., & Van Dyne, L. (2015). *Handbook of cultural intelligence: Theory, measurement, and applications*. Routledge. Ang, S., Rockstuhl, T., & Tan, M. L. (2015). Cultural intelligence and competencies. *International encyclopedia of social and behavioral sciences*, 2, 433-439.

Azevedo, A. (2018). Cultural intelligence: key benefits to individuals, teams and organizations. *American Journal of Economics and Business Administration*, 10(1), 52-56.

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, 101, 1-12.

- Chaho, R. M., Aswad, A. (2021) The Cryptocurrency Legality and Environmental Challenges. *International Journal of Green Management and Business Studies*, Vol. (1), No. (1), Pp. 50-61
- Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, 137, 103614.
- Darwish, S. (2014). Education and Human Capital Development in Bahrain:" Future International Collaboration with Malaysia. *International Journal of Academic Research in Management (IJARM)* Vol, 3, 321-334.
- Englander, M. (2019). General knowledge claims in qualitative research. *The Humanistic Psychologist*, 47(1), 1.
- Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cybersecurity culture framework. *Sensors*, 21(9), 3267.
- Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452-462.
- Hassan, M. A., Ali, S., Imad, M., & Bibi, S. (2022). New Advancements in Cybersecurity: A Comprehensive Survey. *Big Data Analytics and Computational Intelligence for Cybersecurity*, 3-17.
- Ioannou, G., Louvieris, P., & Clewley, N. (2019). A Markov multi-phase transferable belief model for cyber situational awareness. *Ieee Access*, 7, 39305-39320.
- Livermore, D., & Ang, S. (2016). Virtual chaos at worldwide Rx: How cultural intelligence can turn problems into solutions. *Intercultural management—A case-based approach to achieving complementarity and synergy*, 167-173.
- Livermore, D., & Soon, A. N. G. (2015). *Leading with cultural intelligence: The real secret to success*. Amacom.
- Mohamed, H. M. (2021) Green-Economic Constructions Using Composite GFRP Closed Forms. *International Journal of Green Management and Business Studies*, Vol. (1), No. (1), Pp. 1-14
- Sternberg, R. J., & Grigorenko, E. L. (2006). Cultural intelligence and successful intelligence. *Group & Organization Management*, 31(1), 27-39.
- Thomas, D. C. (2008). *Cultural intelligence: People skills for global business*. ReadHowYouWant.com.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- Tongdhamachart, N., & Alwi, A. (2023). The Cultural Identity of Mien Ethnic Group in a Digital Era. *International Journal of Professional Business Review*, 8(1), e01256-e01256.