Assessing The Factors of Cybersecurity Awareness in the Banking Sector

Adel Ismail Al-Alawi[1]* and Sara Abdulrahman Al-Bassam[2]

[1]The University of Bahrain, College of Business Administration, Department of Management and Marketing, Kingdom of Bahrain

[2]College of Graduate Studies, Department of Innovation & Technology Management Arabian Gulf University, Kingdom of Bahrain

*E-mail: adel.alalawi@gmail.com

Abstract

The purpose of this paper is to identify the factors of cybersecurity awareness in the banking sector. Literature shows several gaps that both top management and cybersecurity professionals must close to construct a successful digital institution in the conviction- and assurance-based economy. These gaps indicate four factors, top management commitment and support; budgeting; cybersecurity compliance; and cybersecurity culture. Methodology: A quantitative approach is used with questionnaire analysis. A total of 109 Information Technology (IT) employees completed a self-administrated survey from six Bahraini Islamic retail banks and five Bahraini conventional commercial retail banks. Descriptive analysis with percentage and a simple mean-based ranking of indicators used to analyze the data. Findings reveal the highest mean is 4.28 for security compliance. The lowest mean for Cybersecurity Culture at 4.24 concludes that all the factors are significant for cybersecurity awareness. Respondents strongly agreed with the necessity of these factors in the banking sector. The research limitation due to the insufficient information in the literature regarding the proposed combination of factors recommended. Practical implications for policymakers and cybersecurity specialists: This study provides a vital factor that may help improve policies or guidelines for successful cybersecurity awareness in organizations. To recognize cyber threats, cyber-attacks impact, and how to diminish cyber risk and avoid cyber-crime penetrating their cyberspace. Originality/value fills a gap in the literature to construct a successful digital institution in the conviction- and assurance-based economy. This study helps managers direct and proceed with their daily activities, where maintaining the cybersecurity component is significant. A cybersecurity component is a defense and safeguards the firm's financial information, intellectual properties, and reputation against unauthorized parties. Moreover, the cybersecurity component concerns the organization and the public individuals exposed to cyber threats through their electronic digital media such as smartphones, personal computers, and Internet protocol systems. However, there is insufficient literature on the proposed combination of factors recommended as factors relating to cybersecurity awareness in the banking sector.

Keywords: Cybersecurity Awareness, Top management support, Budget, Compliance, Culture, Crime, Banking sector, Bahrain, Cyber threats, Security risks, Training.

Received: 03/05/2021
Revised: 14/06/2021
Accepted: 24/06/2021

Introduction

The organization's most substantial assets and factors are its workers; this can also be its weakest link in data protection, mainly when mobility and accessibility play an enormous role in improving efficiency. Therefore, the issue of the cybersecurity component is not only a concern for the organization but also to the public individuals who are also exposed to cyber threats through their electronic digital media such as their smartphone, personal computer, and Internet protocol system (Kuhlman & Kempf, 2015; Al-Alawi et al., 2020b).

Staff training is essential in raising awareness among personnel and motivating them to pay attention to cyber threats and counteracting steps, even if they are not part of their role. To safeguard the business from any attack, staff training and engagement are significant in constructing awareness among workers and inspiring them to give attention to cyber threats, with these being the best-known tactics used against future cyber threats (Al-Alawi & Al-Amer, 2006; Bada et al., 2014, Al-Bassam, 2018).

Despite the fact that there are countless studies on cybersecurity issues in the Arab world, there is a lack of studies that focus on awareness of cybersecurity among top-level management, employees, and their attitude. Via education and awareness, all staff can be equipped to act as a human firewall to defend against any attack (Al-Alawi et al., 2016; Kumawat, 2021). This study will mainly focus on cybersecurity awareness (CSA) factors in the Bahraini banking sector, which will be found through previous studies, primarily through the state of cybersecurity implications.

Literature has referred to the insufficiency of CSA among employees within organizations; researchers such as Aloul (2012) have stated that "Security awareness is an often-overlooked factor in an information security program where there is a need for effective information security awareness." Similarly, governments such as the UK government have found that employee error is thought to be the highest cause of data breaches within cybersecurity, with the majority of mishandling of data coming from fundamental human mistakes due to the lack of awareness and training (Palmer, 2016).

The purpose of this research is to assess the factors of the CSA in the Bahraini banking sector. Literature shows several gaps that both top management and cybersecurity professionals must close to construct a successful digital institution in the conviction- and assurance-based economy. These gaps indicate four factors, top management commitment and support; budgeting; cybersecurity compliance; and cybersecurity culture. Figure 1. illustrates the research gap.

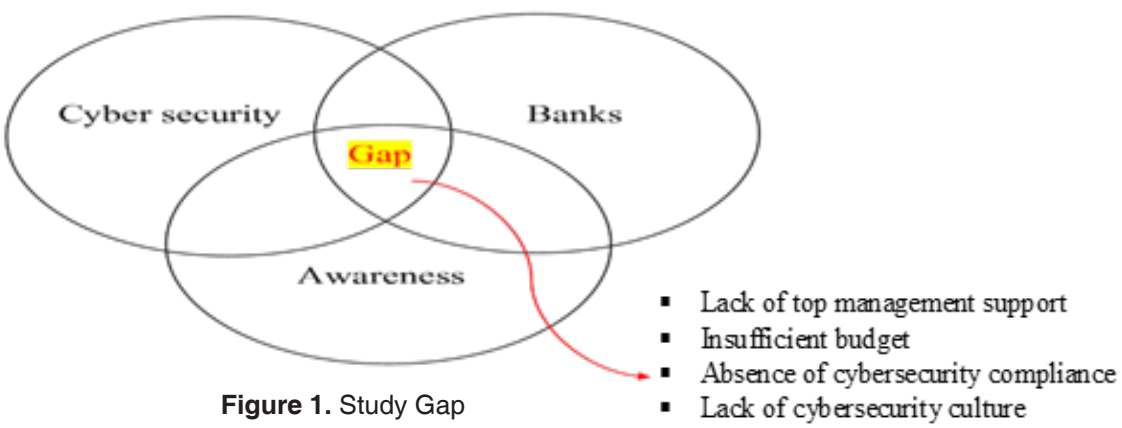

Figure 1. Study Gap

Research Questions

The study will answer the question in order to achieve the goals and objectives of the research. Cybersecurity acts as a process that is designed to defend the organization's computer network and data from various types of attacks in cyberspace.

What are the factors of cybersecurity awareness in the banking sector in Bahrain?

LITERATURE REVIEW

1. Factors of Cybersecurity Awareness

After carefully studying the relevant studies from a large pool of research, this section is based on the survey and the findings of the previous and current studies in relation to the key elements. These factors were not found as a group in any earlier studies to fill the gap in the research.

2. Top Management Commitment and Support

Factor one is concerned with top management commitment and support to developing awareness and the significance of management at different levels to CSA. According to the previous studies, it can be concluded that managers certainly endorse the concept that management commitment and support are imperative for developing a successful awareness program in the financial and banking sector and other sectors (Knapp et al., 2004; Al-Alawi & Al-Amer 2006; Rainer et al., 2007; Al-Alawi, 2006). For example, Alghamdi (2021) and Al-Alawi (2006) emphasized that top management commitment and support is the most crucial factor affecting cybersecurity management activities in institutions.

3. Budget

Factor two is concerned with budgeting. According to Von Solms (1999), this is a crucial factor where management must be convinced about the importance of cybersecurity before providing an adequate budget and acting to impose the cybersecurity policy. Najibzadeh & Park (2021) and Al-Awadi & Renaud (2007) stated that the lack of a proper budget means that institutions cannot be armed with sufficient resources to ensure cybersecurity. Furthermore, the budget is the financial facility, which usually estimates the costs and measures the access required to the resources to implement cybersecurity successfully.

4. Cybersecurity compliance

Factor four is concerned with security compliance; this is vital in decreasing an institution's information security risks (Al-Alawi & Al-Bassam, 2020). ISACA (2015) defined compliance as" the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations. It also includes voluntary requirements resulting from contractual obligations and internal policies". Studies indicate that staff consistently are not aware of the cybersecurity consequences of their activities and do not sufficiently recognize the outcome of their security decisions (Pham et al., 2021). This situation can be addressed if a precise vision from top management is shown to affect the staff's behavior in keeping the institution's information resources through compliance with the security policy (von Solms & von Solms, 2004).

5. Cybersecurity culture

This factor is concerned with finding the significance of CSA that must be initiated from the top management to inspire a crucial attitude from workers and expect them to comply with an institution's security policy rules and regulations. Institutions with shortages of proper resources will face complications in managing some general security issues, for instance, access control mechanisms or assisting workers in requesting beneficial security practices like an automatic logoff or regular password changes. The 2002 security awareness index report cited by McKay (2003) concluded that institutions globally are failing to make their staff aware of the security issues and the consequences.

CSA assists in initiating a culture within institutions, and an influential culture increases the effectiveness of information systems management (Knapp et al., 2006; Pahnila et al., 2007; Puhakainen & Siponen, 2010). The value of creating a security culture within banking institutions results from the fact that the human aspect in information security is continuously measured to be the weakest link (Hadlington, 2021; Da Veiga & Eloff, 2009; Schlienger & Teufel, 2003).

Methodology

A quantitative approach is used with questionnaire analysis. The data were collected from 109 participants out of 168 employees from six Bahraini Islamic retail banks and five Bahraini conventional commercial retail banks to determine the level of cybersecurity awareness in the banking sector. The targeted population consisting of IT managers and those who have IT security job responsibilities. Descriptive analysis with percentage, frequency, and a simple mean-based ranking of indicators used to analyze the data. Five intervals of scale were used to interpret the respondent's degree of agreement.

According to the Central Bank of Bahrain (CBB) , the banking system in Bahrain encompasses both conventional and Islamic banks. It is the primary element of the monetary system, accounting for more than 85% of the entire monetary resources in Bahrain. "The conventional segment includes 23 retail banks, 69 wholesale banks, 2 specialized banks as well as 36 representative offices of overseas banks. The Islamic segment, offering a host of Sharia compliant products and services, includes 6 retail banks and 18 wholesale banks."

The following formula was used to calculate the score intervals:
Score interval = (Maximum score- Minimum score)/ Number of levels
= 5- 1 /5 =0.8
The following Table 1 shows the rating scale used to measure the degree of agreement:

Table 1
Likert Scale of Agreement

1-1.8	1.81-2.6	2.61-3.4	3.41-4.2	4.21-5
Strongly Disagree (SD)	Disagree (D)	Neutral (N)	Agree (A)	Strongly Agree (SA)

Results

The questionnaire was about the factors of CSA in the Bahraini banks. The respondents were requested to show their level of agreement on scale ranking by using a five-point Likert scale, from a score of 1 labeled “strongly disagree” to a score of 5 marked “strongly agree” in considering essential factors related to CSA in the Bahraini banking sector. The analysis uses a simple mean-based ranking of indicators within each construct. Table 2 shows a summary of the factors ranked by the mean. The highest mean is 4.28 for security compliance, and the lowest mean for Cybersecurity Culture at 4.24. The difference between the highest and lowest is 0.04, less than one standard deviation of overall summary 0.152. Such a small variance indicates the importance of all indicators, as mentioned earlier. Additional analysis was conducted to provide more insight into the results.

The following sections present the current state of practice for each of the constructs in Bahraini banks. Hence, the first rank is for cybersecurity compliance at the mean of 4.28, the second rank for top management support at 4.26, the third rank goes for the budget at the mean of 4.25, and the lowest rank is for cybersecurity culture at 4.24.

Table 2

The summary of the factors ranked by the mean

Rank	Factors	Mean	SD*
1	Security Compliance	4.28	0.547
2	Top Management support	4.26	0.495
3	Budget	425	0.628
4	Cybersecurity Culture	4.24	0.476

SD*: Standard deviation

Discussion

Top management support and commitment

This factor measured the importance of top management support for cybersecurity awareness in Bahraini banks. This factor has 12 statements shown in Table 3, with the ranking of mean results.

Table 3

Ranked statements for top management support factor

Rank	Statements	Mean	SD*
1	Support from senior management is essential to secure the resources needed to ensure a security awareness program can achieve its aims.	4.43	0.699
2	Lack of top management support and commitment will increase the possibility of a cybersecurity program failure.	4.38	0.767
3	When creating a cybersecurity culture, commitment and support from the top management and strong leadership is necessary at an initial stage to succeed in the long term.	4.36	0.776
4	Top management commitment and support is an essential part of the establishment of a cybersecurity culture.	4.34	0.723

5	Support and commitment from senior management staff relate to the levels of comprehension regarding cybersecurity's importance held by these key players as well as the range of their involvement in such activities.	4.29	0.761
6	Top management staffs consider cybersecurity an important organizational priority.	4.26	0.787
7	Support from senior management staff holds the most significant influence in cybersecurity culture and enforcement of the organization's policies in this regard.	4.24	0.804
8	Top management staff understands their roles and responsibilities.	4.24	0.719
9	Support and commitment from senior management staff play an essential role as the main element influencing the banking sector's cybersecurity.	4.22	0.712
10	The implementation and sustainable maintenance of cybersecurity awareness among stakeholders require ongoing commitment and support.	4.14	0.763
11	Top management staff gives consistent and robust support to the cybersecurity program.	4.13	0.840
12	The senior management staff is always involved in key cybersecurity activities.	4.06	0.792
	Top management support and commitment total average	**4.26**	**0.752**

*SD: Standard Deviation

Table 3 shows that the average mean value of the statements of this factor ranged between (4.06-4.43), while the values of standard deviation ranged between (.699-.840). The first rank goes to the statement, which stated, "Support from senior management is essential in order to secure the resources that are needed to ensure a security awareness program can achieve its aims," with the highest mean of (4.43) and standard deviation of (.699). The second rank is for the statement, which stated, "Lack of top management support and commitment will increase the possibility of a cybersecurity program failure" with a mean of (4.38) and standard deviation of (.767). The third rank drives the statement, "When creating a cybersecurity culture, commitment and support from the top management and strong leadership are necessary at an initial stage to succeed in the long term," with a mean of (4.36) and standard deviation of (.776). The fourth rank goes to the statement, which stated, "Top management commitment and support is an essential part of the establishment of a cybersecurity culture" with a mean of (4.34) and standard deviation of (.723). The fifth rank is for the statement which stated "Support and commitment from senior management staff relate to the levels of comprehension regarding cybersecurity's importance held by these key players as well as the range of their involvement in such activities," with the mean of (4.29) and standard deviation of (.761). The sixth rank is for the statement, which stated, "Top management staff considers cybersecurity an important organizational priority," with the mean of (4.26) and standard deviation of (.787). Seventh and eighth-ranked equalized and illustrated respectively in sequence with two statements stating, "Support from senior management staff holds the greatest influence in cybersecurity culture and enforcement of the organization's policies in this regard" with the mean of (4.26) and standard deviation of (.804). In addition, "Top management staff understand their roles and responsibilities" for a mean of (4.24) and standard deviation of (.719). The ninth rank is for the statement, which stated, "Support and commitment from senior management staff plays an essential role as the main element that influences banking sector cybersecurity," with the mean of (4.22) and standard

deviation of (.712). The tenth rank goes to the statement, which stated, "The implementation and sustainable maintenance of cybersecurity awareness among stakeholders require ongoing commitment and support," with a mean of (4.14) and standard deviation of (.763). The eleventh rank drives the statement, which stated, "Top management staff gives strong and consistent support to the cybersecurity program" with a mean of (4.13) and standard deviation of (.840). The last rank for this factor is the statement that stated, "Senior management staff is always involved in key cybersecurity activities," with a mean of (4.06) and a standard deviation of (.792).

Result analysis: The top management factor mean average is (4.26). The standard deviation is (.752), which reflects that the respondents strongly agreed that top management support and commitment are essential for CSA.

Budget

This factor measures the importance of a budget for cybersecurity awareness in Bahraini banks; it has nine statements. Table 4 shows the results of this factor.

Table 4

Ranked statements of the Budget factor

Rank	Statements	Mean	SD*
1	A comprehensive budget is essential to ensure appropriate resources are allocated to cybersecurity.	4.48	0.554
2	The bank should properly allocate budget towards training and the smart use of automation to improve detection and automation to improve detection and response capabilities.	4.36	0.601
3	Lack of cybersecurity budgeting in the bank leads to failure to hire professional cybersecurity staff.	4.28	0.695
4	The budget is the financial facility that firstly rationally estimates the costs and secondly assesses access to the resources required to achieve the successful implementation of cybersecurity.	4.24	0.592
5	Depending on the size of your bank, you will need to secure a decent-sized budget to get to started and maintain the cybersecurity program.	4.21	0.625
6	Although information security budgets have increased, boards need to keep close to the strategy to ensure the budget is spent most effectively.	4.21	0.639
7	Lack of cybersecurity budgeting in organizations leads to under-investment inappropriate controls.	4.18	0.611
8	Organizations will need to allocate strategic funding to establish and make commitments to cybersecurity practices in light of the sophisticated attacks seen in recent years.	4.17	0.646
9	The bank is spending appropriately on cybersecurity priorities.	4.14	0.687
	Budget total average	**4.25**	**0.628**

*SD: Standard Deviation

Table 4 shows that the mean value of the statements of this factor ranged between (4.14 4.48-). In contrast, the importance of standard deviation ranged between (.687.-554) with the budgeting factor average of 4.25 and a standard deviation of .628. The first rank applies to the statement, which stated, “A comprehensive budget is essential to ensure appropriate resources are allocated to information security,” with a mean of (4.48) and standard deviation of (.554). The second rank is for the statement, which stated, “The bank should properly allocate budget towards training and the smart use of automation to improve detection and response capabilities” with the mean of (4.36) and standard deviation of (.601). The third rank is for the statement, which stated, “Lack of cybersecurity budgeting in the bank leads to failure to hire professional cybersecurity staff,” with the mean of (4.28) and standard deviation of (.695). The fourth rank goes for the statement, which stated, “Budget is the financial facility, which firstly rationally estimates the costs and secondly assesses the access to the resources required to achieve successful implementation of cybersecurity” with a mean of (4.24) and standard deviation of (.592). Fifth and sixth-ranked equalized and illustrated respectively in sequence with two statements stating, “Depending on the size of your bank, you will need to secure a decent-sized budget to get started and maintain the cybersecurity program” with mean of (4.21) and standard deviation of (.625). And statement which stated, “Although information security budgets have increased, boards need to keep close to the strategy to ensure the budget is spent most effectively,” with the mean of (4.21) and standard deviation of (.639). The seventh rank goes for the statement, which stated, “Lack of cybersecurity budgeting in organizations leads to under-investment inappropriate controls,” with a mean of (4.18) and standard deviation of (.611). The eighth rank is for the statement, “Organizations will need to allocate strategic funding to establish and make commitments to cybersecurity practices in the light of the sophisticated attacks seen in recent years,” with a mean of (4.17) and a standard deviation of (.646) . The ninth rank is for the statement, which stated, “The bank is spending appropriately on cybersecurity priorities,” with the mean of (4.14) and standard deviation of (.687).

Result analysis: The budgeting factor mean for all statements was (4.25), and the standard deviation was (.628), which means respondents strongly agreed with the necessity of a budget for CSA.

Cybersecurity Compliance

This factor measures the importance of security compliance and has ten statements. Table 5 shows the results of this factor.

Table 5
Ranked statements of the cybersecurity compliance factor

Rank	Statements	Mean	SD*
1	I intend to protect information and technology resources according to the requirements of the cybersecurity policy of the bank in the future.	4.43	0.725
2	I am familiar with the potential risks relating to cybersecurity and the resulting damaging consequences.	4.42	0.613
3	I understand the concerns regarding cybersecurity and the risks that banks face.	4.33	0.609

4	My intention is to follow the guidelines of the cybersecurity policy to execute my responsibilities to improve the bank's cybersecurity concerning my IT activities in the future.	4.30	0.752
5	I intend to comply with the requirements of the cybersecurity policy of the bank in the future.	4.28	0.804
6	I know my responsibilities as prescribed in the cybersecurity policy to enhance the cybersecurity of the bank.	4.26	0.738
7	Information assurance is a security technique that encompasses a defense-in-depth strategy composed of three components: technology, operations, and people. The components form the foundation and framework for developing a comprehensive security strategy.	4.26	0.763
8	I understand the rules and regulations prescribed by the cybersecurity policy of my bank.	4.25	0.735
9	Compliance has improved the bank's cybersecurity capabilities.	4.21	0.840
10	I know the rules and regulations prescribed by the cybersecurity policy of the bank.	4.15	0.768
	cybersecurity compliance total average	**4.29**	**0.735**

SD*: Standard Deviation

Table 5 shows that the average mean value of the statements of this factor ranged between (4.15-4.43), while the values of standard deviation ranged between (.609-.840). The first rank goes for the statement, which stated, "I intend to protect information and technology resources according to the requirements of the cybersecurity policy of the bank in the future," with the highest mean of (4.43) and standard deviation of (.725). The second rank is "I am familiar with the potential risks relating to cybersecurity and the resulting damaging consequences," with the highest mean of (4.42) and standard deviation of (.613). The third rank is for the statement, which stated, "I understand the concerns regarding cybersecurity and the risks that organizations face," with a mean of (4.33) and a standard deviation of (.609). The fourth rank drives the statement, which stated: "My intention is to follow the guidelines of the cybersecurity policy to execute my responsibilities to improve the bank's cybersecurity with my IT activities in the future" with a mean of (4.30) and standard deviation of (.752). The fifth rank is for the statement, which indicated, "I intend to comply with the requirements of the cybersecurity policy of the bank in the future," with the mean of (4.28) and standard deviation of (.804). Sixth and seventh-ranked equally and illustrated respectively in sequence with two statements, which stated, "I know my responsibilities as prescribed in the cybersecurity policy to enhance the cybersecurity of the bank," with a mean of (4.26) and standard deviation of (.738). Moreover, the statement stated, "Information assurance is a security technique that encompasses a defense-in-depth strategy composed of three components: technology, operations, and people. These components form the foundation and framework for developing a comprehensive security strategy" with a mean of (4.26) and standard deviation of (.763). The eighth rank goes for the statement, "I understand the rules and regulations prescribed by the cybersecurity policy of my bank," with the mean of (4.25) and standard deviation of (.735). The ninth rank is for the statement stated ,"compliance has improved the bank's cybersecurity capabilities" with the mean of (4.21) and standard deviation of (.840). The last rank goes for the statement, which stated, "I know the rules and regulations prescribed by the cybersecurity policy of the bank," with the lowest mean of (4.15) and standard deviation of (.768).

Result analysis: The average mean for the factor (4.29) and standard deviation (.735) reflect that respondents strongly agreed regarding the security compliance necessary for CSA.

Cybersecurity culture

This factor measures the importance of cybersecurity culture; it has 11 statements, and Table 6 illustrates the results of this factor.

Table 6
Ranked statements of Cybersecurity culture factor

Rank	Statements	Mean	SD*
1	Top management should enforce the cybersecurity program and create a cybersecurity culture within the bank.	4.48	0.661
2	Bank security needs to be implemented from the initial stages to be fully integrated and prevent users from taking a rash approach.	4.41	0.641
3	By increasing the awareness of users, the understanding and improvement of security culture can be accomplished.	4.40	0.668
4	Bank management staff should understand that there are no quick fixes in cybersecurity and that a proper cybersecurity culture must be cultivated within the bank.	4.39	0.639
5	The time and resources that banks spend on implementing advanced technology mean that it is essential to develop a culture of security awareness within the bank to provide the necessary support for this.	4.37	0.676
6	One goal of a cybersecurity organizational culture is to influence the behavior of staff concerning complying with the official security policy.	4.34	0.641
7	A security policy is essential for both the effectiveness of cybersecurity management and the establishment of a security culture.	4.30	0.701
8	The board should play a significant role in driving the IT strategy, given its importance in corporate strategy. This should cover every dimension of the management of technology systems; that is to say: cost, human capital, hardware and software, vendors and service providers, and risk management, including disaster recovery, should be factored in the IT strategy of the bank.	4.12	0.729
9	At most organizations, the Board of Directors plays no part in the main activities relating to cybersecurity.	3.97	0.822
10	Many cybersecurity awareness programs fail to educate the users on why security is crucial and fail to motivate the users to change their behavior.	3.96	0.816
11	The board of directors frequently takes no role regarding essential initiatives, which include security strategy, budget, and risk assessment. This is despite recent security breaches, which attracted a high level of publicity.	3.86	0.833
	Cybersecurity culture total average	**4.24**	**0.712**

SD*: Standard Deviation

Table 6 shows that the average mean value of the statements of this factor ranged between (3.86-4.48), while the values of standard deviation ranged between (.639-.833). The first rank drives the statement, which stated, "Top management should enforce the cybersecurity program and create a cybersecurity culture within the bank," with the highest mean of (4.48) and standard deviation of (.661). The second rank goes for the statement, which stated, "Bank security needs to be implemented from the initial stages, in order to be fully integrated and prevent users from taking a rash approach," with the mean of (4.41) and standard deviation of (.641). The third rank is for the statement, "By increasing the awareness of users, the understanding and improving a security culture can be accomplished," with a mean of (4.40) and standard deviation of (.668). The fourth rank goes to the statement, which stated, "Bank management staff should understand that there are no quick fixes in cybersecurity and that a proper information security culture must be cultivated within the bank," with a mean of (4.39) and standard deviation of (.639). The fifth rank goes for the statement which stated: "The time and resources that banks spend on implementing advanced technology mean that it is essential to develop a culture of security awareness within the organization to provide the required support for this" with the mean of (4.37) and standard deviation of (.676). The sixth rank is for the statement, which stated, "One goal of a cybersecurity organizational culture is to influence the behavior of staff concerning complying with the official security policy," with a mean of (4.34) and standard deviation of (.641). The seventh rank goes for the statement, which stated, "A security policy is important for both the effectiveness of information security management and the establishment of a security culture," with a mean of (4.30) and standard deviation of (.701). The eighth rank is for the statement, "The board should play a significant role in driving the IT strategy, given its importance in corporate strategy. This should cover every dimension of the management of technology systems, that is to say: cost, human capital, hardware and software, vendors and service providers, and risk management, including disaster recovery, should be factored in the IT strategy of the bank" with a mean of (4.12) and standard deviation of (.792). The ninth rank drives the statement, which stated, "At most organizations, the Board of Directors plays no part in the main activities relating to information security" with a mean of (3.97) and standard deviation of (.822). The tenth rank is for the statement, which stated, "Many cybersecurity awareness programs fail to educate the users on why security is important and fail to motivate the users to change their behavior," with a mean of (3.96) and standard deviation of (.816). The last rank goes for the statement, which stated, "The board of directors frequently takes no role regarding important initiatives, which include security strategy, budget, and risk assessment. This is despite recent security breaches, which attracted a high level of publicity" with the lowest mean of (3.86) and standard deviation of (.833).

Result analysis: The cybersecurity culture factor showed an average of (4.24) and a standard deviation of (.712); that means the respondents were strongly agreed that cybersecurity culture requires CSA.

6. Conclusion

The crisis of cybercrimes has been cultivated into a global environment; to elaborate a scientific method of resolving this dilemma. It is crucial to formalize the separation and classification of the key objectives of the critical properties of the matter (Al-Alawi &

Abdelgadir, 2006; Al-Alawi, 2014; Al-Alawi et al., 2020a). Therefore, it is more crucial for an organization to increase its cybersecurity investments and awareness rather than focusing on its technical measures. Hence, organizations must have significant economic relationships with the market to have a good decision-making process. They are required to detect issues and find quick resources to help solve them.

This study concludes that all the factors (Security compliance, Top management commitment and support, Budget, and Cybersecurity culture) are essential for cybersecurity awareness, and respondents strongly agreed with the necessity of these factors. Security compliance ranked first with an average mean of (4.29) and was found to be a vital factor in decreasing an institution's information security risks; reflect those respondents were strongly agreed regarding the security compliance necessary for CSA. Top management commitment and support to developing awareness learned to be significant and ranked second with an average mean of 4.26. Thus, top management support is a crucial factor in supporting the performance of security management and policy. The study also supported the importance of a budget, where management was convinced about the importance of cybersecurity before providing an adequate budget and acting to impose the cybersecurity policy. The budget factor ranked third with an average mean of (4.25) and concerned with the level of top management commitment and support to developing awareness. The next factor four, 'Cybersecurity culture, ranked fourth, with an average mean of (4.24). This is concerned with finding the significance of CSA that must be initiated from the top management to inspire a crucial attitude from workers and the expectation that they will comply with an institution's security policy rules and regulations. This research is limited to cybersecurity, the banking sector, and the Kingdom of Bahrain.

Recommendation and future research

The recommendations of this research are directed towards the improvement of CSA as follows:

- Top management staff should give solid and consistent support to the cybersecurity program.
- Spend appropriately on cybersecurity priorities and invest in appropriate controls.
- To focus on compliance to improve the bank's cybersecurity capabilities.
- The board of directors must play a part in the main activities relating to cybersecurity.

Future research can be extended to include the following:

- Similar analysis on other sectors and industries.
- Further studies on the same factors affecting cybersecurity awareness in other international banks and financial institutions and to compare Bahraini and other Gulf Cooperation Council (GCC) countries banks.

The contribution of this study

The contribution of this study to the scientific community and its economic implications affirm that this study helps managers direct and proceed with their daily activities, where maintaining the cybersecurity component is significant. A cybersecurity component is a defense and safeguards the firm's financial information, intellectual properties, and reputation against unauthorized parties. Moreover, the cybersecurity component is a concern for the organization and the public individuals who are also exposed to

cyber threats through their electronic digital media such as their smartphone, personal computer, and Internet protocol system. However, there is insufficient literature on the proposed combination of factors recommended as factors relating to cybersecurity awareness in the banking sector.

Funding Information
No organization funded this study.

Author Contribution *(statement of responsibility)*
Both authors contributed equally at all stages (Group efforts at all stages).

Conflict of Interest
We would like to confirm that the authors haven't received any financial support, personal relationships, or involvement in any organization or entity with financial or non-financial interest.

References

Al-Alawi, A. I. (2006). Investigating the strategies for successful development of health information systems: A comparison study. *Information Technology Journal*, 5(4), 626-647.

Al-Alawi, A.I & Abdelgadir, M.F. (2006), An Empirical Study of Attitudes and Opinions of Computer Crimes: A Comparative Study between UK and Kingdom of Bahrain, *Journal of Computer Science,* 2(3), 229-235.

Al-Alawi, Adel Ismail and Al-Amer, Mohamad Ahmed (2006), Young Generation Attitudes and Awareness Towards the Implementation of Smart Card in Bahrain: An Exploratory Study, *Journal of Computer Science* 2 (5), 441-446

Al-Alawi, A. I. (2014). Cybercrimes, Computer Forensics and their Impact on Business Climate: Bahrain Status. *Research Journal of Business Management*, *8*(3), 139-156.

Al-Alawi, A. I., Al-Kandari, S. M., & Abdel-Razek, R. H. (2016). Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University. *Journal of Innovation and Business Best Practice*, 2016:1-24.

Al-Alawi, A. I., Mehrotra, A. A., & Al-Bassam, S. A. (2020a). Cybersecurity: Cybercrime Prevention in Higher Learning Institutions. *In Implementing Computational Intelligence Techniques for Security Systems Design (*pp. 255-274). IGI Global.

Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020b). Critical Cybersecurity Threats: Frontline Issues Faced by Bahraini Organizations. *In Implementing Computational Intelligence Techniques for Security Systems Design* (pp. 210-229). IGI Global.

Al-Alawi, A. I. & Al-Bassam, S.A (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector, *Journal of Xidian University, 14(7), 1523- 1536, DOI: http://doi.org/10.37896/jxu14.7/174*

Al-Awadi, M., & Renaud, K. (2007, July). Success factors in information security implementation in organizations. In *IADIS International Conference e-Society*.

Al-Bassam, S.A (2018), Investigating the Factors related to Cybersecurity Awareness in Bahraini Banking Sector,(Master Thesis, Arabian Gulf University (AGU), Salmanya, Kingdom of Bahrain) and supervised by Prof. Adel Ismail Al-Alawi. Unpublished dissertation, available from AGU Library

Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Materials Today: Proceedings*.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183.

Bada, M., & Sasse, A. (2014). *Cyber Security Awareness Campaigns Why do they fail to change behaviour?* (pp. 1-38, Working paper). Global Cyber Security Capacity Centre. *http://discovery.ucl.ac.uk/1468954/1/Awareness CampaignsDraftWorkingPaper.pdf*

Da Veiga, A., & Eloff, J. H. P. (2009). A framework and assessment instrument for information security culture. *Computer & Security*, 1-12.

Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. In Research Anthology on Artificial Intelligence Applications in Security (pp. 1960-1977). IGI Global.

ISACA (2015), "The Cybersecurity Fundamentals Study Guide", ISBN 978-1-60420-594-7

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson-Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.

Knapp, K., Marshall, T., Rainer, R., & Morrow, D. (2004). Top Ranked Information Security Issues. Paper presented at the 2004 International Information Systems Security Certification Consortium (ISC) 2 Survey Results.

Kuhlman, R., & Kempf, J. (2015). "Report on Cybersecurity Practices". FINRA publishes its 2015 *Journal of Investment Compliance*, 16(2), 47-51.

Kumawat, M. K. (2021) Security of Data Science and Data Science for Security.

McKay, J. (2003). Pitching the Policy: Implementing IT Security Policy through Awareness. *USA: SANS Institute*.

Najibzadeh, O., & Park, S. (2021). The Cybersecurity of The Future Nevadans. *Journal of Student Research*, *10*(1).

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In System Sciences, 2007. HICSS 2007. 40Th annual

Hawaii international conference on (pp. 156b-156b). IEEE.

Palmer, D. (2016). Training? What training? Workers' lack of cybersecurity awareness is putting the business at risk. Retrieved 12 December 2016, from: *http://www.zdnet.com/article/training-what-training-workers-lack-ofcyversecurity-awareness-is-putting-the-business-at-risk/*

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.

Rainer Jr, R. K., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do information security professionals and business managers view information security issues differently? *Information Systems Security*, *16*(2), 100-108.

Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice. *Australasian Journal of Information Systems*, *25*.

Schlienger, T., & Teufel, S. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. Paper presented at the DEXA Workshops.

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50-58.

Von Solms., S., & von Solms, R. (2004). The 10 deadly sins of Information Security Management. *Computer & Security*, 23, 371376.

تقييم عوامل الوعي بالأمن السيبراني في القطاع المصرفي

عادل إسماعيل العلوي[1]* وسارة عبدالرحمن محمد البسام[2]

[1] استاذ الإدارة ونظم المعلومات – كلية إدارة الأعمال – جامعة البحرين

[2] مرشح لنيل درجة الدكتوراه كلية الدراسات العليا – جامعة الخليج العربي – البحرين

*بريد الكتروني: adel.alalawi@gmail.com

المُستَخلَص

تاريخ استلام البحث: 2021/05/03
تاريخ تعديل البحث: 2021/06/14
تاريخ قبول البحث: 2021/06/24

الغرض من هذه الورقة هو تحديد عوامل الوعي بالأمن السيبراني في القطاع المصرفي. تظهر الأدبيات العديد من الثغرات التي يجب على كل من الإدارة العليا ومحترفي الأمن السيبراني إغلاقها لبناء مؤسسة رقمية ناجحة في الاقتصاد القائم على الاقتناع والضمان. تشير هذه الفجوات إلى أربعة عوامل، التزام ودعم الإدارة العليا، الميزانية، الامتثال للأمن السيبراني، وثقافة الأمن السيبراني. المنهجية: تم استخدام الأسلوب الكمي حيث أكمل 109 موظفًا في مجال تقنية المعلومات تعبئة الاستبانات من ستة بنوك تجزئة بحرينية إسلامية وخمسة بنوك تجزئة بحرينية تقليدية. وقد تم تحليل الاستبانات وصفيا خلال حساب النسب المئوية والمتوسط الحسابي لكل عامل. تظهر النتائج أن أعلى متوسط هو 4.28 للامتثال للأمن السيبراني وأدنى متوسط لثقافة الأمن السيبراني عند 4.24 وتم التوصل إلى أن جميع العوامل مهمة للوعي بالأمن السيبراني. وافق المستطلعون بشدة على ضرورة وجود هذه العوامل في القطاع المصرفي. تبرز محددات البحث بسبب عدم كفاية المعلومات الواردة في الأدبيات المتعلقة بالمجموعة المقترحة من العوامل. النتائج العملية: توفر هذه الدراسة عوامل فعاله قد تساعد واضعي السياسات والمتخصصين في الأمن السيبراني في تحسين السياسات أو الإرشادات من أجل الوعي الناجح بالأمن السيبراني في المنظمات. للتعرف على التهديدات الإلكترونية وتأثير الهجمات الإلكترونية وكيفية تقليل المخاطر الإلكترونية وتجنب اختراق الجرائم الإلكترونية للفضاء الإلكتروني الخاص بهم. تكمن الأصالة / القيمة لهذه الورقة بسد فجوة الأدبيات لبناء مؤسسة رقمية ناجحة في الاقتصاد القائم على الاقتناع والضمان. تساعد هذه الدراسة المديرين على توجيه أنشطتهم اليومية والمضي قدمًا فيها، حيث يكون الحفاظ على الأمن السيبراني أمرًا مهمًا. الأمن السيبراني هو وسيلة دفاع لحماية المعلومات المالية للشركة، والملكية الفكرية، والسمعة ضد الأطراف غير المصرح لها. علاوة على ذلك، يتعلق الأمن السيبراني بالمنظمة والأفراد العاملين المعرضين للتهديدات السيبرانية من خلال الوسائط الرقمية الإلكترونية مثل الهواتف الذكية، أجهزة الحاسوب الشخصية وأنظمة بروتوكول الإنترنت. ومع ذلك، لا توجد دراسات كافية حول المجموعة المقترحة من العوامل الموصي بها كعوامل تتعلق بالوعي بالأمن السيبراني في القطاع المصرفي.

الكلمات الدالة: الكلمات الرئيسية - الوعي بالأمن السيبراني، دعم الإدارة العليا، الميزانية، الامتثال، الثقافة، الجريمة، القطاع المصرفي، البحرين، التهديدات السيبرانية، المخاطر الأمنية، التدريب.